Defending the Digital Fortress:

Safeguarding Cell Phone Privacy in Civil Litigation

by Robert S. Stickley and Connor J. Thomson

Based on a hypothetical sorority hazing incident, this article explores the legal and policy implications of a digital forensic examination of an insured's cell phone during discovery. It delves into privacy, cybersecurity, burden, cost, and attorney-client privilege concerns, framing the discovery demand as an "electronic strip search." Drawing on legal precedents and offering five practical tips for insurance defense attorneys and claims professionals, the authors propose filing a motion for protective order to secure the insured's personal privacy and dignity and to prevent unwarranted financial burdens on the insurance industry.

Imagine that you are defending a claim involving allegations of sorority hazing.

The incident resulted in serious injuries and was the subject of a criminal investigation by the university and local police. Your insured, a member of the sorority, is being sued and defended pursuant to her parents' homeowners insurance policy.

During discovery, the plaintiff's attorney propounds hundreds of interrogatories and requests for production of documents upon your insured, some of which demand access to the data on your insured's cell phone. Specifically, the plaintiff's attorney demands that your insured surrender her cell phone to a digital forensic examiner for extraction of all data (both deleted and saved) from a certain time period.

Should your insured also be subjected to an electronic strip search at the whim of an opportunistic plaintiff's attorney? We think not. The discovery demand triggers a multitude of concerns, including privacy, cybersecurity, burden, cost, and attorney-client privilege.

The Electronic Strip Search

Cell phones are ubiquitous and necessary in modern society. Oftentimes, we cannot work, shop, see a doctor, or attend a concert without one. Yet, we seldom consider that the most significant—and intimate—aspects of our lives are contained in these handheld electronic devices.

Further, the amount of "deleted" data that remains hidden deep within our cell phones is staggering. In the span of just a few hours, a talented digital forensic examiner can recover thousands of text messages, emails, images, and browsing histories that were deleted years ago—or so we thought.

The founders of our great nation certainly did not imagine the existence of cell phones when they crafted the Fourth Amendment, which protects citizens from illegal government searches and seizures . However, in a seminal 2014 case, *Riley v. California*, the United States Supreme Court stated that we must interpret the Fourth Amendment to include electronic devices,[1] reasoning that

"it is no exaggeration to say that many of the more than 90 percent of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[2]

Since the Supreme Court's decision in *Riley*, other federal courts have acknowledged that a digital forensic examination of a cell phone is a "drastic discovery measure"[3] that, if not safeguarded against, may provide a plaintiff's attorney access to "the most personal and intimate facts"[4] of a defendant's life.

Cell phones include private and intimate thoughts and images shared with loved ones, banking, health, and medical information, work assignments, goals, aspirations, feelings (happy and depressed), and GPS locations. Also, and often overlooked, if you are involved in a lawsuit, your cell phone includes your strategy for defending the lawsuit in the form of attorney-client communication. As courts are now beginning to acknowledge, cell phones are vastly different than any other physical item; they are "simultaneously offices and personal diaries," but with immense storage capacity.[5]

This is precisely why the Ninth Circuit in the *United States v. Cotterman* equated a digital forensic examination of an electronic device to a "computer strip search."[6] Because "an individual has a reasonable expectation of privacy in its cellular telephone records,"[7] "such a thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity."[8]

Just because cell phones allow people to hold information in their hands doesn't mean they are less deserving of the protection the founders sought.[9] Our judicial system recognizes that defendants have an undisputed right to personal privacy and dignity. Allowing a plaintiff's attorney to peer into the most private realm of a modern-day defendant undermines "the founders' deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion."[10]

At the same time, circling back to the hypothetical at the beginning of this article, if you are defending a claim involving allegations of sorority hazing, you cannot ignore the reality that your insured's cell phone may contain information relevant to the subject lawsuit.

Practice Tips

So how do you balance privacy, cybersecurity, burden, cost, and attorney-client privilege concerns with the obligation to comply with what may be an overzealous discovery demand? One way is to file a motion for protective order after doing some advanced planning.

In the example presented, if the circumstances permit, you should (1) document your insured's good faith compliance with her discovery obligations, (2) have a firm understanding of the governing rules, (3) be familiar with the case law, and (4) craft a strong policy argument. Doing so will hopefully forestall the plaintiff's attorney from taking advantage of your insured and costing the insurance industry thousands of dollars.

Practice Tip No. 1: Document

A plaintiff's attorney is trained to create a record before seeking a court order for a digital forensic examination. This record consists of proof that the plaintiff's attorney

“The founders of our great nation certainly did not imagine the existence of cell phones when they crafted the Fourth Amendment, which protects citizens from illegal government searches and seizures”

(1) requested the preservation of nonprivileged data at the earliest stage of litigation, (2) requested the nonprivileged data as part of its initial request for production of documents, and (3) inquired about how the defendant communicated (i.e., the electronic device and mobile application used) during the deposition.

Consequently, in the case at hand, documenting, and including in your motion for protective order, your insured's good faith compliance with her discovery obligations is paramount. If you can demonstrate that your insured diligently responded to, and fully participated in, discovery without willful default, the court may be more receptive to your argument.

Practice Tip No. 2: Firmly understand the governing rules

The Federal Rules of Civil Procedure permit "discovery regarding any non-privileged matter that is relevant to any party's claim . . . ," including electronically stored information (ESI).[11] However, they limit the frequency and extent of discovery so that it's:

> ...proportional to the needs of the case, considering the importance of the issues at stake . . . , the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and *whether the burden or expense of the proposed discovery outweighs its likely benefit.*[12]

Most states' Rules of Civil Procedure are akin to the language of the federal rules and bar discovery, including ESI discovery, when information "is sought in bad faith" [13] or "would cause unreasonable annoyance, embarrassment, oppression, *burden, or expense."* [14]

So in the sorority case, you should be prepared to demonstrate to the court that the ESI is not discoverable because of undue burden or cost. If your motion for protective order demonstrates that undue burden and cost, there is a good chance you "need not provide discovery" of the ESI.[15]

Practice Tip No. 3: Be familiar with the case law

The case law from most jurisdictions suggests that (1) discovery is not without limits,[16] and (2) courts have "wide discretion to deny discovery."[17]

For example, courts have wide discretion to deny discovery when a plaintiff's attorney requests an unfettered inspection of an opponent's computer system, as "the creation of forensic image backups should only be sought in exceptional circumstances."[18] And even in such circumstances—for example, if a defendant has willfully defaulted on its discovery obligations—a court should only allow "restrained and orderly computer forensic examinations."[19]

Unrestrained and unorderly computer forensic examinations are impermissible because there is a need to "guard against . . . intrusiveness."[20]

When navigating issues regarding cell phone privacy and electronic strip searches, you should delve into both civil and criminal case law to build a comprehensive understanding of the legal landscape. Examining criminal case law can provide insights into how courts interpret and apply privacy laws in the context of searches and seizures, wiretapping, and electronic surveillance.

Practice Tip No. 4: Craft a strong policy argument

The most important part of your motion for protective order is your policy argument. Judges, like everyone else, are human beings and can be influenced by their own experiences and perspectives. Despite the goal of objectivity, in some situations, emotions play a role in judicial decision making.

To craft the strongest policy argument, remember to be mindful of the weight of authority and cite the supreme law of the land—the Fourth Amendment. You should consider advocating for robust privacy protections that strike a balance between individual rights and legitimate investigative needs. Additionally, arguing for clear guidelines on when and how electronic strip searches can be conducted, with a focus on minimizing intrusiveness and respecting personal privacy and dignity, could be a compelling policy stance.

Practice Tip No. 5: Tactically address costs and logistics

You should educate the court regarding the science involved with extracting data from your insured's cell phone. We recommend that you provide an affidavit from the digital forensic examiner explaining how deleted data (yes—those uber-secret text messages, emails, images, and browsing histories we would never want our grandparents to see) remains on cell phones for years. This affidavit should also outline the costs and suggest that the plaintiff should have to pay for compliance.

A second affidavit from your insured can help build a record demonstrating that your insured's cell phone contains private and intimate thoughts and images shared with loved ones, banking, health, and medical information, and attorney-client communications about the subject lawsuit. This affidavit should also outline your insured's burdens, costs, and anxieties associated with her not having access to her cell phone for several days.

The goal, of course, is to prove that the discovery demand for your insured's cell phone extraction is outweighed by privacy, cybersecurity, burden, cost, and attorney-client privilege concerns. The court must understand that surrendering the cell phone is a really big deal to the insured and could lead to a series of horrible and unintended consequences.

Financial Burdens on the Insurance Industry

If the opportunistic plaintiff's attorney succeeds with its discovery demand, the discovery demand will increase an insurance company's loss adjustment expenses, thereby also increasing its loss ratio.

Speaking from experience, digital forensic investigation companies bill insurance companies between $300 to $475 per hour to take custody of one cell phone and extract data of interest. The minimum amount of time for imaging a cell phone is three hours.

If the subject lawsuit is litigated to verdict, expert testimony is billed at $4,500 per day. And that does not include a $3,500 retainer, expert reports, opinion letters, affidavits, declarations, certifications, or reasonable and necessary expenses for travel, tax, computer equipment, shipping, and delivery.

At its scope, insurance is the act of risk transfer and distribution. When insurance companies pool their risks, the risk pools evenly share all losses and loss adjustment expenses. So, when insurance companies experience an increase in loss adjustment expenses, the expenses are passed on to every insured in the form of higher premiums.

A United Defense

The challenges posed by the hypothetical at the beginning of this article demand a vigilant response by the insurance industry.

The primary responsibility of an insurance defense attorney is to protect its insured in the name of justice. This includes protecting the insured's personal privacy and dignity. By leveraging a motion for protective order, an insurance defense attorney can shield its insured from undue intrusion, thwart opportunistic attempts to exploit the discovery process, and serve as a bulwark against potential misuse of litigation tactics that could have broader financial effects .

For insurance defense attorneys reading this article, we hope that you use this strategy as a roadmap in your own practice. For insurance claims professionals reading it, we hope that you use this strategy as a checklist for your panel counsel. Together, we can, and will, defend the digital fortress. ■

For more information on this topic, please contact Robert S. Stickley at rstickley@stickley.law or Connor J. Thomson at cthomson@stickley.law

1. See *Riley v. California*, 573 U.S. 373 (2014).
2. *Id.* at 395 (citing *Ontario v. Quon*, 560 U.S. 746, 760 (2010)).
3. *Tingle v. Hebert*, No. 15-626-JWD-EWD, 2018 U.S. Dist. LEXIS 60301, at *19 (M.D. La. Apr. 10, 2018).
4. *Lawson v. Love's Travel Stops & Country Stores, Inc.*, No. 1:17-CV-1266, 2020 U.S. Dist. LEXIS 3352, at *7 (M.D. Pa. Jan. 9, 2020).
5. *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013).
6. *Id.* at 966.
7. *Commonwealth v. Benson*, 10 A.3d 1268, 1272 (Pa. Super. Ct. 2010).
8. *Cotterman*, 709 F.3d at 968.
9. See *Riley*, 573 U.S. at 403.
10. *United States v. Seljan*, 547 F.3d 993, 1014 (9th Cir. 2008) (Kozinski, C.J., dissenting).
11. Fed. R. Civ. P. 26(b)(1).
12. *Id.* (emphasis added).
13. Pa. R. Civ. P. 4011(a).
14. Pa. R. Civ. P. 4011(b) (emphasis added).
15. Fed. R. Civ. P. 26(b)(2)(B).
16. See *Banks v. Beard*, No. 3:CV-10-1480, 2013 U.S. Dist. LEXIS 99905, at *5 (M.D. Pa. July 17, 2013).
17. *McNeil v. Jordan*, 894 A.2d 1260, 1274 (Pa. 2006).
18. *Valdes v. Greater Naples Fire Rescue Dist.*, No. 2:17-cv-417-FtM-29CM, 2018 U.S. Dist. LEXIS 152744, at *13 (M.D. Fla. Sept. 7, 2018).
19. *Landau v. Lamas*, No. 3:15-CV-1327, 2017 U.S. Dist. LEXIS 206158, at *14-15 (M.D. Pa. Dec. 15, 2017) (collecting authorities).
20. *John B. v. Goetz*, 531 F. 3d 448, 460 (6th Cir. 2008).