FOLEY

FOLEY & LARDNER LLP

Text Messages, EDiscovery, and the New Threat to Privacy

Maybe some of you will look at the title of this article, smirk, and dismissively mutter that there is nothing new about text messages. eDiscovery practitioners also may think there is nothing revolutionary about considering text messages (or counterpart means of communications through WhatsApp and similar systems) as fair game in eDiscovery. And that would be true. Courts have been requiring text message preservation and production for the last several years. *See, e.g., Nuvasive, Inc. v. Madsen Medical Inc.*, 2015 WL 4479147, at*1-2 (S.D. Cal. July 22, 2015) *sanction decision amended* 2016 WL 305096 (S.D. Cal. Jan. 26, 2016). Moreover, for family law and personal injury practitioners, text messages (and social media postings) have long been fertile grounds for harvesting evidence of infidelity, harassment, and fraud. *See, e.g.*, Laura M. Holson, "Text Messages: Digital Lipstick on the Collar." New York Times, Dec. 8, 2009. But something seems different now. For business lawyers and the attorneys who represent them, what was the occasional is becoming more and more mainstream. Just as we say to clients, "We are going to need to collect company emails," we now are saying, more and more, "We are going to need people's cell phones."

And a great hue and cry was heard throughout the land. Or there will be one in the near future.

How did we get here? We will assume a general understanding of the history of written communication as it passed from primitive rock carving to scribing on papyrus scrolls to the eventual development of paper and ink. But, come the mid-1980s, a seismic shift occurred. Paper gave way to electronic communications, and the world of emails exploded upon the business (and legal) community. Over the course of the next 10-or-so years, hard-copy paper records –letters, memoranda, customer files, etc. – began disappearing while emails and electronic documents surged forward. Document review moved from collecting and physically handling hundreds or thousands of boxes of hard-copy documents to computer-screen review of millions of emails and e-docs.

At first we printed out all the emails to review (really, we did!), but with the change in technology came the "eDiscovery vendor" and the birth of electronic review platforms and a myriad of tools to make review more manageable and reliable. We lawyers learned about metadata, TIFFing, native productions, back-up tape rotations, de-duping, hash-tagging, email threading, clustering, structured data, file shares, archiving, auto-purges, and a host of other technical challenges and solutions. The Federal Rules of Civil Procedure formally recognized the change that had occurred with its 2006

amendments that coined the term "ESI" ("Electronically Stored Information"), and over the last decade or so we have been busy refining how to handle eDiscovery. Generally, however, we've got this down now, and what was once daunting has become routine.

Clients, too, have come far in terms of their understanding about the needs and breadth of eDiscovery. In the early years, there was much consternation about the idea of collecting employees' emails and letting lawyers have free rein to review them. There was employee teeth gnashing about having to turn over "personal" folders, "private" emails, collections of "jokes" or, indeed, hordes of material of a more . . . *ahem* . . . erotic nature. (Oh, yes, there was *much* of that.) Eventually, with experience and the introduction of updated and explicit corporate communication policies, employees began to understand that what they had regarded as "private" on their work computers was not private at all and subject both to corporate and legal review. Companies also introduced training programs so that employees, from the most junior to the most senior levels, were taught that they should never put in an email words that they would not want to see blasted in a news article or show up as evidence in a courtroom. These lessons were learned, sometimes the hard way (or the *really* hard way), but they were learned nonetheless, and a new norm emerged.

Now we are at a new tipping point, as a younger generation rises in the business community, and smartphones and smart technology pervade all aspects of our lives. According to the Pew Research Center, as of 2015, millennials – generally those born between 1981 and 1996 – had become the most prominent generational group in the American workforce. Richard Fry, Pew Research Center, https:// www. pewresearch. org /fact-tank/2018/04/11/millennials-largest-generation-us-labor-force/. To that generation, texting became second nature. Meanwhile, the iPhone, Android devises, and other smart phone counterparts have now become ubiquitous – indeed, even "elderly" baby boomers are devotees. What does this convergence mean? As a recent article in The American Lawyer explained "Clients are Saying Goodbye to Email, and Lawyers are Forced to Adapt." Rhys Dipshan, *The American Lawyer*, www.law.com / americanlawyer / 2019/10/03. We also see headlines such as "When These Executives Want Candid Advice, They Text." Chip Cutter, *Wall Street Journal*, Oct. 14, 2019. High-level government officials also have joined the crowd. As recent news stories reported, a former senior White House adviser warned superiors that the U.S. Ambassador to the EU was a counterintelligence risk because he extensively uses his personal cell phone to text and communicate with others in the diplomatic community. Nicholas Fandos and Adam Goldman, "Ex-Aid Saw Gordon Sondland as a Potential National Security Risk," *New York Times*, Oct. 16, 2019. It is a near certainty that Ambassador Sondland is not unique among government officials in this context. *See, e.g.*, John Hudson and Karoun Demirjian, "Clinton-Email Critics Pull a Role Reversal as Trump Administration Draws Fire for Private Phone Use," *Washington Post*, October 9, 2019.

The thing is that texting is just so easy. So quick. You can do it from anywhere, anytime. No need to devote precious time to the arduous task of typing an email address and a subject line, as called for by email. So old school! And texts from a personal cell phone are private. Right? Uh . . . no. This is where the privacy issue comes in, and a whole lot of people are going to be very surprised and unhappy.

There are, indeed, companies and governmental entities that issue mobile phones – smartphones – for use in conducting company or official business. For users of such devices, the right and ability of a company, and its lawyers, to obtain all data from those phones, including text messages, is no different from collecting emails from a company computer system. Courts have

recognized this right.[1] *See, e.g., Rightchoice Managed Care, Inc. v. Hospital Partners, Inc.*, 2019 WL 3291570, at *2 (W.D. Mo. July 22, 2019) (granting motion to compel text messages from senior employees' business-issued cell phones); *Lalumiere v. Willow Springs Care, Inc.*, 2017 WL 6943148, at *2 (E.D. Wa. Sept. 18, 2017 (company controls employees' text messages from company phones and must produce responsive texts); *Stinson v. City of New York*, 2016 WL 54684, at *5 (S.D.N.Y Jan. 5, 2016) (police officers' city-issued smartphones subject to preservation obligations; text messages should have been preserved).

But what of business-related text messages sent entirely on a person's private phone? This is where the law is evolving and where a window into the "private" world of communications is opening more and more. As of 2014, the Supreme Court recognized that "[M]odern 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.'" *Riley v. California*, 573 U.S. 373, 403 (2014).

So, what happens if you use your personal cell phone to text others about business matters – regardless of whether your intent was to make those statements "in private" or whether you did so just as a matter of convenience? In *Matthew Enterprise, Inc. v. Chrysler Group LLC*, 2015 WL 8482256, at *3-4 (N.D. Cal. Dec. 10, 2015), the court denied a request to obtain defendant's employees' emails from their personal computers on the grounds that the corporate defendant did not have possession or control over the employees' personal accounts. This same analysis has been applied to text messages from personal cell phones. *See, e.g., RightChoice Managed Care*, 2019 WL 6943148, at *2 (W.D. Mo. July 22, 2019) (text messages from non-party employees' personal phones not discoverable); *Lalumiere*, 2017 WL 6943148, at *2 (company does not possess or control text messages on its employees' personal phones).

Other courts have taken a different approach. In *H.J. Heinz Co. v. Starr Surplus Lines Ins. Co.*, 2015 WL 12791338, at *4 (W.D. Pa. July 28, 2015), the court accepted the sworn statements of two key Heinz employees, that they did not use their personal cell phones "related to substantive Heinz business" but ordered Heinz to interview their 10-12 other document custodians to determine if they used their personal cell phones to text about substantive, relevant topics and, if so, to produce those texts to defendant. *Id.*

The court, in *Royal Park Investments SA/NV v. Deutsche Bank National Trust Co.*, 2016 WL 5408171, at *5-6 (S.D.N.Y. Sept. 27, 2016), considered a request to obtain relevant emails from plaintiff's Board members' non-company email accounts. Following a long line of decisions from the Southern District of New York judges, the *Royal Park* judge noted that the possession-and-control analysis extended to whether a party had the "practical ability" to obtain ESI from a non-party. For example, courts will ask whether the corporate party has the ability to fire an employee for non-compliance with a request to obtain documents/ESI from a personal devise. *Id.* (citing *Chevron Corp. v. Salazar*, 275 F.R.D. 437, 448-49 (S.D.N.Y. 2011)). Other indicia are whether the non-party has a fiduciary responsibility to turn over documents, maintains an ongoing economic relationship with a party, or has acted as an agent for the party. *Id.* At a very minimum, the New York line of cases expect a party to ask either its employees or a non-party to produce the relevant material. *Id.*

The Delaware Chancery Court has taken a similar approach, as shown in a suit brought by the former founder, Board member, and CEO of Papa John's pizza, who was seeking texts from other Board members' private cell

[1] In identifying certain cases, the author is not taking a position on the merits of the various decisions.

phones relating to his ouster after he made controversial statements about NFL players protesting the national anthem. There, the court noted that texts often provide probative information and that if the company's other directors, CEO, and general counsel used personal devises to communicate about ousting the founder "they should expect to provide that information" as requested. *Schnatter v. Papa John's Intern'l Inc.*, 2019 WL 194634, at *16 (Del. Ct. Chan. Jan. 15, 2019).

OK. It seems pretty clear that text messages from private cell phones are discoverable, at least in some courts, and the number of such courts is very likely to increase in the coming years, especially as texting for business purposes becomes even more common. Now, the real issue – and the one that should cause a sharp intake of breath by those who jealously guard their privacy – is the collection of those texts. Why? Because most often collection requires the phone to be surrendered to a "vendor" representative for at least a few hours. "*Who? What?*" Yes, document custodians are almost certainly going to wind up handing their personal phones – their personal electronic lifeblood to the universe – to a complete stranger for hours at a time so that their information can be "extracted." The attorney who makes this announcement to the document custodians should be prepared for all sorts of invective-strewn tantrums to ensue, and may wish to wear body armor when attempting to take possession of the phone. (Okay, the latter may be a slight exaggeration – but only slight.) Meanwhile, in all candor, some sophisticated eDiscovery vendors have developed the ability to arrange for "remote" extraction, but that technology is still rare and developing. Moreover, such remote collections are usually only able to extract "live" texts, not deleted ones. Likewise, it is sometimes possible to obtain text messages through iCloud via iTunes – but again deleted texts cannot be captured with this method.

By the way, something else that the phone's owner should understand: the extraction will not be limited to "relevant" text messages. Such refined extracting and searching is not possible with text messages – at least not yet. Rather, *all* information available on the phone will be "extracted." That's right – not only *all* the texts, but *all* the photos, *all* the regular websites visited and searched, *all* the phone numbers called and *all* the phone numbers of in-coming calls, and *all* the other "privacies of life" teeming within the electronic brains of the individual's smartphone.

The technology available for extracting data from cell phones continues to advance at a rapid pace. Just a few years ago, eDiscovery vendors struggled with being able to download text messages and then provide them in a format that a human being could read. Often the best that was possible was to present the text exchanges in a spreadsheet format. Some people would just take screen shots of their text messages and hand over those static, non-searchable pictures of their texts. *See, e.g., Herzig v. Ark. Found. For Med. Care, Inc.*, 2019 WL 2870106, at *4, (W.D. Ark. July 3, 2019). (Apparently, taking screen shots of text messages is easy – as long as you have a 14-year-old readily available and you don't mind a disdainful eye roll when you ask for help. If that's too painful, you can also go to Google or YouTube for instructions.) Today, eDiscovery vendors and software technology developers have caught up, at least to some degree, and are able to extract smartphone information and upload the data to a document review platform such as Relativity. They, however, are in a race with the smartphone technologists who, in turn, are seeking to convince a dubious public that they have included new features designed specifically to guard a user's privacy. This tension between the two technology fields is not going to abate.

Another challenge that has arisen with extracting and rendering text messages is that it is now possible to include Emojis, Animoji, Stickers, Effects, Handwriting, Digital Touch (Apple Watch), and Tapback as part of the message. (No, I *don't* know what all of those

are, either.) Even assuming that the data can be captured and provided in a readable format, imagine the interpretation difficulties in deciphering emoji facial expressions, let alone when a facial image is followed by images of some activity, food, sports paraphernalia, etc. Bottom line: Text extraction is going to become ever more complicated with each new feature.

But the real concern is privacy. Will all this extraction from a personal cell phone mean that, as texting becomes more and more the norm in the business arena, a person's entire personal smartphone life will become available for lawyer to review and produce? The answer should be a qualified "no," based on both technical practicalities and recent judicial decisions.

First, just because an eDiscovery vendor extracts all the phone's data, lawyers can instruct, for example, that the vendor provide them only with texts exchanged with certain business contacts' numbers, thereby limiting review to potentially relevant exchanges and avoiding examination of spouse-to-spouse, parent-to-child, and other private, personal, and completely irrelevant text exchanges. Of course, in cases involving things such as fraud, misappropriation, insider trading, and various other claims of malfeasance, a wider search to additional cell phone numbers may become necessary, given people are more likely to bury such contacts among their other mundane text messages. Such expanded searches are possible because even if attorney review initially is limited to certain business contacts' cell phone numbers, the vendor will retain the full extraction (unless instructed otherwise). Hmmm . . . . Along those lines, once a matter is concluded, an attorney should instruct the vendor to destroy any retained copies of data collected, whether from a company's email servers, a business-issued smartphone, or an individual's personal cell phone.

Second, the courts have put limitations on overly zealous efforts to strip away a person's private communications. In *Tingle v. Hebert*, 2017 WL 2536584, at *4-5 (M.D. La. June 9, 2017), the court considered a motion to compel in which defendant sought all text messages exchanged from plaintiff's personal phone between plaintiff and employees of the agency that defendant oversaw. The court found that such a request was overbroad and not proportional to the needs of the case. *Id.* at *4. Rather, the court instructed that the request should be limited to text messages within a certain time period and only on specific topics relevant to the claims in the suit. *Id.* at *5. This decision is similar to the decisions in *H.J. Heinz Co. and Schnatter*, where the courts permitted discovery of texts from personal cell phones but limited production to texts on relevant topics. Consistent with this line of cases, very recently in *Hardy v. UPS Ground Freight, Inc.*, 2019 WL 3290346, at *3-4 (D. Mass. July 22, 2019), the court denied a motion to compel seeking a forensic examination of plaintiff's personal cell phone on the grounds that such an examination threatened to sweep in plaintiff's private information and that the motion contained no proposed protocol "appropriately tailored to protect [plaintiff's] privacy concerns." *Id.* at *3.

Perhaps the most interesting case to confront this issue is *Laub v. Horbaczewski*, 331 F.R.D. 516 (C.D. Cal. 2019). There, in a breach of contract case, text messages and iNotes were collected from defendant's iPhone and produced in discovery. However, the production consisted of spreadsheets of the texts that inadvertently were produced prior to being reviewed for relevance, privilege, and privacy concerns. Among those text messages were communications between defendant and some of the company employees, one of defendant's college friends who was also a potential investor in the company, and about 3,700 texts with a company human resources employee with whom defendant was having a romantic relationship. *Id.* at 518. *Gulp*. Upon discovering the error, defendant's counsel sought for the production to be returned and

offered to produce a substituted version with redactions for irrelevance, privilege, and "privacy." The judge conducted an *in camera* review of the entire original production and ultimately determined that, even though defendant inadvertently produced texts that contained irrelevant communications, there was no legal basis to permit a party to "claw-back" ESI solely on relevance grounds. Therefore, the court decided that any substitute production had to include all such irrelevant texts. *Id.*

But . . . but, as to the thousands of irrelevant texts of a romantic nature, the court noted that federal courts recognize a constitutional right to privacy encompassing a right to nondisclosure of one's personal information. *Id.* In such cases, production will depend on balancing the need for the information against the particular private information disclosed. *Id.* The court then canvassed various decisions throughout the country where privacy concerns relating to, for example, financial information, special needs accommodations, and tax information, were found to outweigh discovery obligations or at least were deemed worthy of special protective order treatment. *Id.* at 522-23. Based on this line of case, the *Laub* court found that the 3,700 text messages reflecting the irrelevant romantic relationship need not be reproduced and that the "seriousness of the invasion of privacy for the individuals involved outweighs any countervailing interest there might be in discovery." *Id.* at 524. The same rationale did not apply, however, to the irrelevant texts between defendant and his college buddy/potential business investor because the level of privacy concerns in those communications were not as high as those raised by the "intimate" romantic texts . *Id.* at 525

So one court has drawn a line. What remains to be seen is whether other courts will follow suit and basically recognize that there is privacy, and then there is *p-r-i-v-a-c-y*. As business-related text message productions, in particular from private cell phones, become more and more the norm, and possibly overtake email productions in the coming few years, the line between what is responsive and what is private surely will face additional challenges. The ultimate lesson is, don't think for a minute that what you text from your own phone will definitely remain hidden away from view and the prying eyes of opposing counsel. What you text is there to discover.

Melinda F. Levitt is a partner in the Washington, D.C. office of Foley & Lardner LLP and practices in the areas of antitrust and complex litigation, with a particular focus on eDiscovery matters. *The author would like to thank the forensic specialists from Transperfect Legal Services and iDS Solutions, Inc. for their technical assistance in the drafting of this article.* *Foley & Lardner's Privacy, Security & Information Management practice provides a depth of practical insights to current privacy issues, including GDPR and CCPA compliance. We also regularly counsel clients on managing and continuously evolving their cybersecurity compliance programs and in responding to and managing the risk of security incidents and breaches.*