E-DISCOVERY

Craig Ball

E-Discovery Update

By Craig Ball

Contents

Never have lawyers enjoyed more ways to answer the questions, "what happened and why?" The world teems with sensor-laden, networked devices informing abundant apps. Once-ephemeral actions and communications are routinely recorded, ready to illuminate intent and serve as Boswell to behavior. Interaction and information on demand have changed us. We stand astride physical and virtual worlds, often more engaged with distal persons than with those at our table. Instant information gratification renders no question too trivial to Google and no attitude or experience insufficiently trenchant to share on Facebook.

Some despair that privacy is gone, the President tweets, and there's no "ducking and covering" from a cyberattack. But, as lawyers doggedly pursuing facts, we can rejoice. The digital universe is paying attention and stands ready to clue us in. All we must do is know where to look, ask the right questions and be tenacious seeking answers.

If you've paid close attention to e-discovery, then the landscape of e-discovery at the start of 2018 looks much like it did when the amended federal rules that kicked in at the close of 2015 were a source of uncertainty, particularly as to proportionality and sanctions. With a longer view, it's clear that proportionality is a blunt instrument, and not all courts are bowing to limits on their power to sanction spoliation of electronically stored information (ESI).

Proportionality

Proportionality describes the sensible proposition that the burdens of discovery shouldn't outweigh its benefits vis-à-vis the needs of the case. The 2015 amendments to Rule 26 of the

Federal Rules of Civil Procedure shifted the elements of proportionate discovery—residing elsewhere in the rule for 30+ years—into the scope of discovery; *viz.*:

> Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense **and proportional to the needs of the case, considering the importance of the issues at stake in the action, 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. Information within this scope of discovery need not be admissible in evidence to be discoverable.**
>
> *FRCP Rule 26(b)(1),* amended language in bold.

Proportionality is routinely (and inarguably) advocated as, "a $50,000 case shouldn't prompt discovery costing $100,000.00." Of course, it shouldn't; but, the parties rarely hold the same view of a case's value or their exposure. As well, the significance of a case cannot always be measured in monetary terms. Consequently, proportionality has manifested after the amendments as (improperly) a boilerplate objection and as (usefully) an analytical framework by which courts issue protective orders according to their sound sense of fairness and discretion. The wise practitioner must couch objections and responses in the elements of the amended Rule, recognizing that courts will be prone to treat those elements as a checklist.

Texas' Take: Calling proportionality the "pole star" informing the exercise of discretion over electronic-discovery disputes, the Texas Supreme Court recently laid out the Texas proportionality factors and pronounced them "in line" with federal counterparts, stating, "[A]ll discovery is subject to the proportionality overlay embedded in our discovery rules and inherent in the reasonableness standard to which our electronic-discovery rule is tethered." *In Re State Farm Lloyds, Relator*, Nos. 15-0903, 15-0905 (Tex. Sup. Ct. May 26, 2017).

The Texas proportionality factors read a bit differently than the federal factors and are "certainly not exclusive." Per *In Re State Farm Lloyds,* Texas looks at:

1. Likely benefit of the requested discovery;
2. The needs of the case;
3. The amount in controversy;
4. The parties' resources;
5. Importance of the issues at stake in the litigation;
6. The importance of the proposed discovery in resolving the litigation; and
7. Any other articulable factor bearing on proportionality.

Spoliation Sanctions

Lawyers approach e-discovery with less enthusiasm than one brings to a root canal. Only the stick of sanctions has served to force litigators to preserve and produce ESI. Courts are loathe to issue sanctions and have done so in only the most egregious circumstances involving the intentional destruction of relevant ESI. Still, parties and counsel unskilled in e-discovery worried that their negligent destruction of evidence might serve as the basis for serious sanctions, like summary dismissal or an adverse inference instruction to the jury. A split between the federal circuits arose over whether serious sanctions could be grounded on negligence or required proof of prejudice and/or malevolent intent, *e.g.*, the Second Circuit required proof of negligence and prejudice where the Fifth Circuit required a showing of bad faith to underpin serious sanctions.

In 2015, the committee charged with drafting the Federal Rules of Civil Procedure sought to resolve the split by amending Rule 37 to limit the ability of judges to sanction the loss and destruction of electronic evidence unless specific requirements are met. FRCP Rule 37(e) now states:

> **If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:**
>
> **(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or**
>
> **(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:**
>
> **(A) presume that the lost information was unfavorable to the party;**
>
> **(B) instruct the jury that it may or must presume the information was unfavorable to the party; or**
>
> **(C) dismiss the action or enter a default judgment.**
>
> *FRCP Rule 37(e),* as amended 2015.

Note the threshold inquiries:

a. Was ESI lost? The amended rule doesn't change anything for the loss of non-electronic items, like paper records or tangible evidence.
b. Should the lost ESI have been preserved for the litigation?
c. Was the ESI lost because reasonable steps weren't taken to preserve it?
d. Can the lost ESI be restored or replaced?

When all these criteria are met, the Rule lays out two exclusive paths:

1. If the lost ESI prompts prejudice to "another" party (presumably the *requesting* party), the Court may order curative measures minimally necessary to offset the prejudice,
   OR
2. If it is determined that the spoliator "acted with the intent to deprive" another party of the use of the ESI in the litigation, the Court may impose serious sanctions *(i.e.*, adverse presumption, adverse inference or dismissal/default).

The amended Rule was intended to occupy the field in terms of ESI spoliation sanctions; but not all judges accept that their inherent, discretionary power to sanction spoliation has been curtailed. *Cf., Cat3 LLC v. Black Lineage, Inc.,* No. 14 Civ. 5511 (AT) (JCF) (S.D.N.Y. January 12, 2016) and *Hsueh v. N.Y. State Dep't of Fin. Servs.*, No. 15 Civ. 3401 (PAC), 2017 WL 1194706 (S.D.N.Y. Mar. 31, 2017).

Texas' Take: The Texas Supreme Court lately weighed in on standards governing spoliation in *Brookshire Bros., Ltd. v. Aldridge*, –S.W.3d–, 2014 WL 2994435 (Tex. July 3, 2013), holding that an adverse inference instruction for spoliation may only be given to a jury when the destruction of evidence was intentional or deprived the opposing party of "any meaningful ability to present a claim or defense." The court added that "[s]poliation findings—and their related sanctions—are to be determined by the trial judge, outside the presence of the jury, in order to avoid unfairly prejudicing the jury by the presentation of evidence that is unrelated to the facts underlying the lawsuit" and that "evidence bearing directly upon whether a party has spoliated evidence is not to be presented to the jury except insofar as it relates to the substance of the lawsuit."

Forms of Production

Lawyers continue to long for the days of paper records and memoranda in red rope folders, and why not? Litigation was simple when you could carry the case file in a briefcase. But, while the legal profession adapted to the demise of typewriters and carbon paper, it clings to the delusion that discovery can be printed out as pixels or ink.

Twenty-first century evidence is principally data, not documents. Accordingly, the forms in which we receive ESI determines if it's utile and complete. Strikingly, lower cost and recognition of native production's superior utility and completeness have driven a slow, sure move away from conversion of ESI to so-called "static" forms of production. If diminished utility and completeness were not sufficient justification to make smart designations of forms of production, the markedly increased per-gigabyte cost paid vendors to ingest and host flabby static formats called "TIFF images" should give any lawyer pause. Poorly-chosen forms of production are not the biggest contributors to the high cost of e-discovery as inefficient approaches to review are most costly, but waste occasioned by the failure to designate, obtain and utilize native and near-native forms of production is still substantial and one of the easiest to fix.[1]

[1] Native forms of production are the same forms the data occupies in the ordinary course of business. It's the form that information takes when the witnesses create and use it. Near-native forms are those which preserve those elements of functionality and completeness as can reasonably be achieved when it's infeasible to produce in

Texas' Take: In federal practice, squabbles over forms of production have become rarer as counsel are less prone to squander energy and goodwill seeking to convert spreadsheets, presentations and other rich formats into static TIFF images over an opponent's objection. Unfortunately, the trend toward efficiency and lower cost has been set back in Texas by the Supreme Court's decision in *In Re State Farm Lloyds, Relator*, Nos. 15-0903, 15-0905 (Tex. Sup. Ct. May 26, 2017). [2]

In a mandamus action seeking to overturn a court's order requiring native forms of production be employed, and despite the plain language of Texas Rule of Civil Procedure 196.4, the Texas Supreme Court held that "neither party may dictate the form of electronic discovery. The requesting party must specify the desired form of production, but all discovery is subject to the proportionality overlay embedded in our discovery rules and inherent in the reasonableness standard to which our electronic-discovery rule is tethered. The taproot of this discovery dispute is whether production in native format is reasonable given the circumstances of [the] case. Reasonableness and its bedfellow, proportionality, require a case-by-case balancing of jurisprudential considerations, which is informed by factors the discovery rules identify as limiting the scope of discovery…." *Id.*

The Court could have recognized that native formats are those used in the ordinary course and, accordingly, are the original evidence as used every day by the parties. Production in native (or, when infeasible, near-native format) is inherently reasonable absent a showing of undue burden or cost because native format is, by definition, the form in which the data is found, as it ordinarily exists in the producing party's systems. Requiring that forms of production be litigated on proportionality grounds according to the circumstances of each case will serve to slow resolution and increase the cost of litigation for all, versus a default rule that parties produce in the forms in which they ordinarily hold the responsive data absent an agreement or order to supply alternate forms.

Cross Border Discovery

If you've lawfully engaged in e-discovery from persons and companies residing within the European Union, you've surely bumped up against the EU's 1995 Data Protection Directive

native forms. That is, an e-mail may need to be converted from a native container format to a near-native single message format. What makes the latter format near-native is that the form selected retains the essential elements that allow an e-mail application to process the data as e-mail.

[2] DISCLOSURE: I served as an expert witness for the homeowners in the case. The homeowners prevailed in terms of resisting mandamus; however, the Texas Supreme Court lost an opportunity to point the way toward lower cost and more efficient e-discovery for all litigants, instead grafting a ponderous analytical framework onto what should be one of the simplest processes in e-discovery. Requiring requesting parties to show cause why evidence should *not* be degraded from the forms used in the ordinary course of business to static forms places the burden on the wrong party. As well, requiring a special showing to demand metadata integral to the original evidence is akin to requiring production of the consonants in a document but demanding good cause be shown to obtain the vowels.

(Directive 95/46/EC) regulating the "processing" of personal data of EU citizens. "Processing" includes collection, retrieval, transmission, use and disclosure—essentially, every action attendant to e-discovery. Moving data to the United States once implicated a regulatory regime of self-certification called the Safe Harbor Principles. In October 2015, the European Court of Justice ruled that the Safe Harbor regime provided an inadequate level of data protection, and one year ago, the European Commission adopted the EU-US Privacy Shield framework (effective July 12, 2016) to enable U.S. companies to more easily receive personal data from EU entities. That said, the viability of the Privacy Shield has been thrown in doubt by President Donald Trump's issuance of an Executive Order on January 25, 2017, requiring that U.S. privacy protections extend only to citizens and permanent residents of the U.S.

As if there weren't enough confusion attendant to cross-border discovery, effective May 25, 2018, the 1995 Data Protection Directive will be supplanted by a new set of data privacy standards called the GDPR for "General Data Protection Regulation" (Regulation 2016/679). The GDPR broadens privacy protections for EU citizens, including a right of explicit consent to processing of personal data and a right to request erasure of personal data. Notwithstanding the optimism of some commentators, the GDPR seems certain to make it more difficult and, accordingly, more expensive to conduct e-discovery from sources based in the European Union. Of course, the EU is just one of several regions around the world that place widely-varying and onerous hurdles in the path of U.S. e-discovery. It won't be as simple as getting the Court to order production when to do so subjects a party to criminal or civil penalties in other jurisdictions.

Cybersecurity and Privacy

Cybersecurity and personal privacy are real and compelling concerns. Whether we know it or not, virtually everyone has been victimized by data breach. Lawyers are tempting targets to hackers because lawyers and law firms hold petabytes of sensitive and confidential data. Lawyers bear this heady responsibility despite being far behind the curve of information technology and arrogant in dismissing their need to be more technically astute. Cloaked in privilege and the arcana of law, litigators have proven obstinate when it comes to adapting discovery practice to changing times and threats, rendering them easy prey for hackers and data thieves.

Corporate clients better appreciate the operational, regulatory and reputational risks posed by lackluster cybersecurity. Big companies have been burned to the point that when we hear names like Sony, Target or Anthem, we may think "data breach" before "electronics," "retail" or "health care." The largest corporations operate worldwide, so are subject to stricter data privacy laws. In the United States, we assume if a company owns the system, it owns the data. Not so abroad, where people have a right to dictate how and when their personal information is shared.

Headlines have forced corporate clients to clean up their acts respecting data protection, and they've begun dragging their lawyers along, demanding that outside counsel do more than pay

lip service to protecting, *e.g.*, personally-identifiable information (PII), protected health information (PHI), privileged information and, above all, information lending support to those who would sue the company for malfeasance or regulators who would impose fines or penalties.

Corporate clients are making outside counsel undergo security audits and institute operational and technical measures to protect company confidential information. These measures include encryption in transit, encryption at rest, access controls, extensive physical security, incident response capabilities, cyber liability insurance, industry (*i.e.*, ISO) certifications and compulsory breach reporting. For examples of emerging 'standards,' look at the Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information lately promulgated by the Association of Corporate Counsel.

Forcing outside counsel to harden their data bulwarks is important and overdue; but, it's also disruptive and costly. Many small firms will find it more difficult to compete with legal behemoths. Savvier small firms, nimbler in their ability to embrace cybersecurity, will frame it as a market differentiator. At the end of the day, firms big and small must up their game in terms of protecting sensitive data.

Enhanced cybersecurity is a rising tide that floats all boats.

Well, maybe not *all* boats. Let me share who's likely to get swamped by this rising tide: *requesting parties (*or, as corporations call them *"plaintiffs' lawyers"),* and their *experts* and *litigation support providers*. Requesting parties and others in the same boat will find themselves grossly unprepared to supply the rigorous cybersecurity and privacy protection made a condition of e-discovery.

Again, *cybersecurity and personal privacy are real and compelling concerns*, but these security concerns will also be used tactically to deflect and defer discovery. They will serve as hurdles and pitfalls tending to make plaintiffs' lawyers think twice before pursuing meritorious cases. If you haven't run into this, you soon will, and your instinct may be to resist. *Don't.*

Fighting to be cavalier about data security is a battle that requesting parties cannot win and should not fight. Requesting parties must instead be ready to put genuine protections in place and articulate them when challenged.

I know some will say, "all we have to do is sign a protective order." But they don't see the trap set by executing protective orders without the ability (and sometimes without the intention) to meet the obligations of the order. High profile gaffes will follow, and the failure of a few will be the undoing of many.

A protective order isn't the answer if it's an empty promise. Requesting parties can't agree to employ stringent data protection and then go about business as usual: e-mailing confidential data, storing it on unencrypted media and failing to ensure that all who receive confidential data from counsel handle it with requisite caution.

Here's how it will go down for some prominent plaintiffs' lawyer:

1. Producing parties will demand protective orders imposing stringent, but appropriate, data protection practices and breach reporting requirements.

2. Requesting parties will sign these orders because—let's be frank—requesting parties will agree to almost anything if they believe it will get them "the smoking gun." Plus, how do you persuade a judge that she shouldn't issue a protective order when all the other side wants are sensible measures like access controls, encryption and breach reporting to protect sensitive data and PII?

3. Requesting parties will treat information produced in discovery with the same care they bring to their own confidential information, which is to say, not much and less than that protective orders typically require.

4. Confidential data will be mishandled, probably with so little actual prejudice as to prompt requesting counsel to ignore the breach reporting obligation in the order, reasoning "no harm, no foul."

5. The breach will ultimately come to light, opening counsel's mishandling of produced data to scrutiny and prompting discovery about discovery. The failure to set up secure systems, establish policies, train employees, test and audit processes and require contractors and experts to do the same will be gleefully dissected in court.

6. The producing party will beat its chest in lamentations of irreparable harm. The legal press will have a field day. The judge will be wrathful. The requesting party's counsel will look like a clown and might lose his ability to serve on plaintiffs' steering committees.

7. Producing parties will ceaselessly argue the now-proven hazard of e-disclosure, and requesting parties everywhere will be tarred with the same brush, challenged to prove they aren't going to be the next ugly breach. Judges will be less willing to grant full and fair discovery and more willing to impose arduous conditions for access.

A cynical and dystopian prediction? Perhaps. But don't imagine it won't happen. It's happening now.

The way to keep this in check is for requesting parties to act now to prepare to receive and protect confidential data sought in discovery.

Requesting parties cannot expect to be held to a lesser standard of cybersecurity than the producing parties compelled to surrender confidential data to them. A grizzled trial lawyer once warned me, "*Defendants are forgiven several lies. Plaintiffs get none*." So, a party can be incautious with its own data because it's theirs; but counsel who fail to protect an opposing party's confidential data will be harshly judged. They don't just hurt their clients and opponents; they undermine the very foundations of discovery.

So, what must counsel for requesting parties do? Here are a dozen suggestions:

1. Take cybersecurity duties seriously. It's not someone else's job. It's your job. You are the gatekeeper. This is Rule One, not by accident.

2. Don't just treat an opponent's confidential data with the care you afford your own; treat it better. It's like money in your trust account. You don't treat client monies/data like your own. You don't commingle client monies/data with yours, and you don't use that money/data for anything but permissible purposes with careful recordkeeping.

3. If there's a protective order, read it closely and be sure you fully understand what it obliges you to do in terms of the day-to-day conduct of any who access confidential information.

4. A proper chain of custody is essential. You must be ready to establish who received confidential data and the justification for its disclosure. You must be able to prove you had a good faith basis to believe that the person receiving confidential data understood the need to protect the data and possessed the resources, training and skill to do so. This obligation encompasses anyone who gets the data from you, including experts, clerical staff, associated counsel and service providers. Anyone with access to confidential data must be well-prepared to protect the data because their failure is your failure.

5. Proceed with caution when disclosing confidential data to experts. Industry experts serve multiple masters and may seek to exploit confidential data obtained in one matter in other engagements. Secure the expert's written commitment not to do so, and enforce it. Additionally, don't supply confidential data to an expert without first obtaining the expert's consent to receive and protect it. People who appreciate the burden of protecting other people's sensitive data want to hold as little of it as possible.

6. Recognize that you don't get to decide what data warrants protection. The designation rules. If you think something isn't properly designated as confidential or sensitive, challenge the designation; but, until the other side concedes or the Court rules, the designation sets the duty.

7. Confidential data should be encrypted in transit and at rest. This means that none of the confidential data gets attached to an e-mail, moved to portable media (*e.g.,* a thumb drive or a portable hard drive) or uploaded to the cloud *unless it is encrypted.* No exceptions. No excuses. BTW, if you store or transmit the decryption keys alongside the encrypted data, it's doesn't count as encrypted.

8. Perimeter protection isn't enough. The biggest risks to confidential data are internal threats, that is, from a craven or careless member of your own team. Trust but verify. Access to confidential data should be afforded only on an as-needed/when-needed basis.

9. Access to confidential data must be monitored and logged, as feasible. Remote access and after-hours access should be audited. Safeguard the other side's confidential data in much the same manner as banks protect the contents of safety deposit boxes: There is physical security (walls, doors, alarm systems and guards) and monitoring of the perimeter (cameras and key cards). There's a vault to keep all contents safe when the perimeter is breached, and access controls to make contents available only to authorized persons (dual-keyed boxes and ID/signature scrutiny). Data protection also incorporates elements of perimeter security (limiting physical access to the devices and systems), monitoring (logging and auditing), a vault (strong encryption with sound key management) and access controls (two-factor login credentials and user privilege management).

10. Have a written data security and incident response policy and protocol in place and *conform your practice to it.* Be sure all employees with access to sensitive and confidential data agree to be bound by the policy, and train everyone in proper cybersecurity. You must first recognize a risk to be prepared to meet it. "No one told me to do that" is not the testimony you want to hear when your staff take the stand.

11. Be wary of oppressive obligations to destroy or "return" data when a case concludes. Confidential case data tends to seep into mail servers, litigation databases, document management tools and backup systems. Are you prepared to shut down your firm's e-mail and destroy its backup media because you failed to consider what an obligation to eradicate data would really entail? Have you budgeted for the cost of eradication and certification when the case concludes?

12. Consider cloud-based storage and review tools that integrate encryption, two-factor authentication and access logging. The cloud's key advantage lies in a user's ability to shift many of the physical and operational burdens of cybersecurity to a third-party. It's not a complete solution, but it serves to put a secure environment for confidential data within reach of firms of all sizes.

If this sounds like a big, costly pain, you're paying attention. It's a headache. It slows you down, and the risks grow and change as fast as the technology. But if requesting parties don't put adequate protections in place on their own, courts will allow producing parties to dictate what hoops requesting parties must jump through to obtain discovery–if, indeed, courts don't deem the risk so disproportionate that they deny access altogether.

E-discovery is hard enough. Don't make it harder by giving opponents the ability to claim you can't be trusted to protect their information.

Technology-Assisted Review

Technology-Assisted Review or TAR is the use of computers trained by lawyers to distinguish between responsive and non-responsive ESI. Properly implemented and tasked to the right sort of ESI, it works more quickly, affordably and reliably than an army of human reviewers looking at

every potentially relevant item. It is an existential threat to the costly, customary and wildly error-prone approach firms typically take to large-scale document review.

Even as I write that, I know you won't believe it. Yet, it's true. The devil is in the details.

In the last few years, the use of TAR has grown markedly, but quietly. TAR still has the aura of a science experiment. Many who have used TAR tools to speed review are reluctant to disclose same lest their methodology be scrutinized. That's the catch-22 with TAR: lawyers trust it enough to use it, but not enough to stand behind it. Perhaps because they don't understand TAR well enough to defend it, or perhaps because they just don't trust it themselves. Likely, they would claim that having to defend TAR would be so costly and time-consuming that it would defeat the point of using it. So, they clam up or claim it's "work product" and refuse to confirm or deny its use.

Recent efforts by the Duke EDRM to set standards for TAR deployments are likely to embolden lawyers and courts to use TAR to speed e-discovery and lower costs. Several courts have approved the use of TAR, but none have required its use…yet. Inevitably, the merits of TAR will prompt a court to require its use when alternate methods are be shown to be too slow, costly or unreliable.

Mobile Goes Mainstream

Can anyone doubt the changes wrought by the modern "smart" cellphone? My current home in New Orleans sits at the corner of one-way streets, my porch a few feet from motorists. At my former NOLA home, my porch faced cars stopped for a street light. From both vantage points, I've seen drivers looking at their phones, some so engrossed they failed to move when they could. Phones impact how traffic progresses through controlled intersections in every community. We are slow-moving zombies in cars.

Distracted driving has eclipsed speeding and drunken driving as the leading cause of motor vehicle collisions. Walking into fixed objects while texting is reportedly the most common reason young people visit emergency rooms today. Instances of "distracted walking" injury have doubled every year since 2006. Doing the math, 250 ER visits in 2006 are over half a million ER visits today, *because we walk into poles, doors and parked cars while texting*.

Look around you. CAUTION: *This will entail looking up from your phone.* How many are using their phones? At a concert, how many are experiencing it through the lens of their cell phone cameras? How many selfies? How many texts? How many apps?

Lately I've begun asking CLE attendees how many are never more than an arm's length from their phones 24/7. A majority raise their hands. These are tech-wary lawyers, and most are Boomers, not Millennials.

Smart phones have changed us. Litigants are at a turning point in meeting e-discovery duties, and lawyers ignore this sea change at peril. The "legal industry" has chosen self-deception when it comes to mobile devices. It's a lie in line with corporate bottom lines, and it once found support in the e-discovery case law and rules of procedure. But, no more.

Today, if you fail to advise clients to preserve relevant and unique mobile data when under a preservation duty, you're committing malpractice.

Yes, I used the "M" word, and not lightly.

I wouldn't have called it malpractice a few years ago. But two things have changed, and we can't hide our heads in the sand. These are paradigm shifts.

The two things are, first, the data on phones and tablets are *not* just copies of information held elsewhere. Mobile data is unique, and often relevant, probative evidence. Second, the locking down of phone content has driven the preservation of mobile content from the esoteric realm of computer forensics to the readily accessible world of apps and backups. These developments mean that, notwithstanding the outdated rationales lawyers trot out for ignoring mobile, the time has come to accept that mobile is routinely within the scope of preservation obligations.

Too, lawyers need to stop treating mobile devices like biohazards and realize that there are easy, low-cost ways to preserve relevant mobile content *without taking phones away from users.* Because it's easy and cheap to preserve it, mobile content is accessible, and its preservation, when potentially relevant, is proportionate under the Rules.

That's a strong stand, and one some will angrily reject. I get where they're coming from. It was wonderful to be able to ignore mobile in e-discovery. Mobile was a black hole. It wasn't just that you had to hire technical experts to use expensive tools to preserve the contents of phones; it was like pulling teeth to get users to let loose of their devices for the hours or days it took to collect them. Even when they did hand them over, more than a few users claimed to have entered the wrong password too many times and "accidentally" wiped the contents of the phone. "Oops. My bad."

If that never happened to one of your clients, it may be because your client wasn't preserving phone data, indulging in the assumption that whatever they'd glean from the phone would be collected elsewhere. They deemed mobile redundant.

Lecturing about mobile and IoT in D.C. last year, an associate from a megafirm confided to me that his firm routinely advised all its litigation clients that they need not preserve the content of mobile devices because "all the relevant content would be duplicated on the servers." I asked if the firm had ever tested its advice against the relevant data to determine if there was truth in what they were telling clients. He admitted they never had and offered that they'd never do so. The firm didn't want to know the facts because the fairy tale of "replicated elsewhere" was what the client wanted to hear.

Is it a fairy tale? I have my own views based on my own comparisons of mobile content versus other collected sources. What I see demonstrates that the claim that what's relevant on a phone is preserved elsewhere is a whopper. I am routinely finding examples of relevant data stored on mobile devices that is not found among the other sources of data routinely preserved in e-discovery. The replication fairy tale is a relic of a bygone era of Blackberry Enterprise Servers and phones with lower IQs than the brilliant devices now our constant companions and confidantes.

But, I'm not asking you (or courts) to take my word for it. *Test it yourself.*

If you're going to tell the tale, then get some metrics to make it plausible. Use sampling. Process the phones of a few key custodians and compare all the potentially relevant items collected from their mobile devices against the other sources collected for the sampled custodians. What's the differential? Is the unique evidence from the mobile device probative and material?

I've done that, and so I know replication is a fairy tale. If you want to claim it's true *for your client in your case*, how about putting some facts to work? Bear the burden of proof, or start bearing the onus of truth. When you have the facts, you'll have to let loose of the legend and preserve relevant mobile content.

That's the bad news for those who would prefer to ignore mobile. But take heart, as that will seem like great news compared to the next development. Yet, there's a silver lining. Mobile preservation's become quick, cheap and easy.

A few years ago, mobile phones shared some of the characteristics of personal computers in that they held latent data that could be recovered using specialized tools sold for princely sums by a

couple of shadowy tech companies. So, the preservation of mobile devices slipped into the shadows, too. Phones and tablets were *forensic* evidence, and only forensic examiners could collect their contents.

Although users used mobile devices all day, the contents of mobile devices were dubbed "not reasonably accessible." It was too costly and burdensome to preserve a phone. Good thing, because users were holding onto their phones tighter than Willie Nelson clutches a bong. Users protested, *"My mobile phone is the only way the kids' school can reach me in an emergency, and I can't use another phone because everyone texts now, and WHO REMEMBERS PHONE NUMBERS ANYMORE?"*

So, the next altered paradigm: In e-discovery today, the forensic-level preservation of phones—the sort geared to deleted content and forensic artifacts—is a fool's errand. As the public learned from the FBI's tussle with Apple over unlocking the iPhones of the San Bernardino terrorists, modern smart phones are locked down hard. Content is encrypted, and even the keys to access the encrypted content are themselves encrypted. Phone forensics isn't what it used to be. More and more, we can't get to that cornucopia of recoverable forensically-significant data.

At the same time, it's quick, easy and free for a user to generate a full, unencrypted backup of a phone without surrendering possession. The user can even place the backup in a designated location for safekeeping by counsel or IT. Will this be a "forensic image" of the contents? Strictly speaking, no. But as the phone manufacturers tighten their security, "forensic imaging" becomes less and less likely to yield up content of the sort encompassed by a routine e-discovery preservation obligation. Not every case is a job for C.S.I.—and I say that as someone who makes a living through computer forensics.

I grant that a full unencrypted backup of an iPhone isn't going to encompass all the data that might be gleaned by a pull-out-all-stops forensic preservation of the phone. But so what? As my corporate colleagues love to say, "*the standard for ESI preservation isn't perfect.*" I always agree adding, "*but it isn't lousy either.*" Preserving by backup isn't perfect; but it isn't lousy. I've come to regard it as sufficient and proportionate. It's good *enough*, and in most cases, darn good.

I think this is important. It's a game changer for what most litigants are doing today. In a view I hope will come to be shared by all who think it through—preservation of mobile device content must become a standard component of a competent preservation effort except where the

mobile content can be shown to be beyond scope. Mobile content has become so relevant and unique, and the ability to preserve it so undemanding, that the standard must be preservation.

Automated and Hosted Processing and Review

The accepted e-discovery workflow has long involved the collection of data by technical personnel and its delivery into the hands of an e-discovery service provider who would process the data into images and generate load files holding extracted text and metadata. These images and extractions would then be loaded into the law firm's "review platform," a tool that mated the extracted text with its corresponding page image and facilitated search and tagging of the collection by multiple reviewers. This approach made it hard to quickly assess a case (because it took a lot of time and money to get the ESI in front of reviewers) and rendered e-discovery too complex or costly for small- and mid-size firms (who would have to make a significant capital investment in review software, servers and workstations.

Lately, the cloud and the development of automated workflows in cloud-based Software-as-a-Service or "SaaS" tools has made it possible for lawyers and support personnel with little technical savvy and no capital investment to upload, process, review and create production sets on a pay-as-you-go basis. Typically charging per gigabyte of data, the cloud service provider processes the data to, *inter alia,* extract its contents and eliminate duplicate items. All processing is done in the cloud, and users pay the host provider monthly (again, typically, on a per gigabyte basis) to rent storage space and access the hosted data. Automated systems allow users to upload data and initiate processing themselves, at any time of day or night.

By standardizing processes, automating workflows and eliminating personnel costs, hosted discovery service providers can offer sophisticated e-discovery services at historically low prices. Though not the optimum approach for very large data sets or unconventional file types, automated and hosted processing and review promises to make e-discovery feasible and affordable in more matters.

Consolidation

Another trend that shows no sign of abating is the consolidation of e-discovery software and service providers as companies gobble each other up. A decade ago, fear, intimidation and technical incompetence made lawyers and clients easy prey for e-discovery vendors charging premium prices. Everyone charged a fortune, so everyone—particularly the service providers themselves—assumed that's what e-discovery costs (*i.e.*, a bundle) and the gravy train would run forever. Price gouging was aided by systematic pricing obfuscation, making apples-to-apples comparisons difficult. Over time, buyers of e-discovery services came to see how much those offerings were merely commodities, and the bottom fell out of the market as sellers embarked on a death race to the bottom on pricing. The result has been that providers—including some of

the biggest names in the industry--had to fold their tents and sold out to their competition in dozens of face-saving mergers.

Fortunately for consumers, consolidation has yet to prompt price increases; however, slim margins and commoditization still plague the survivors, who continue to collapse into one another at a rate of attrition not offset by startups. It's a buyers' market for e-discovery; but, it behooves the buyer to understand what they are getting.

Attorney Competence

After years trying to persuade lawyers to acquire the barest technical fundamentals of e-discovery, I never cease to marvel at the ingenuity and compelling arguments my trial lawyer colleagues use to explain why they shouldn't need to know this "e-stuff." But, no thanks to me, the battleship is turning in other states, and a conversation has started about the need to equip the next generation of lawyers with the technical knowledge they need to thrive in an era when all information is digital and all evidence electronic. In 2015, California issued a formal ethics opinion requiring that counsel involved in matters involving electronically-stored information to either 'learn it, get help or get out.' The opinion sets out nine skill sets that lawyers dealing with e-discovery must possess or be obliged to decline the representation. The Opinion notes that an attorney handling e-discovery matters, either by themselves or in association with competent co-counsel or expert consultants, should be able to:

- Initially assess e-discovery needs and issues, if any;
- Implement/cause to implement appropriate ESI preservation procedures;
- Analyze and understand a client's ESI systems and storage;
- Advise the client on available options for collection and preservation of ESI;
- Identify custodians of potentially relevant ESI;
- Engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan;
- Perform data searches;
- Collect responsive ESI in a manner that preserves the integrity of that ESI; and
- Produce responsive non-privileged ESI in a recognized and appropriate manner.

The State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2015-193.

Likewise, the state of Florida now mandates that that its lawyers obtain three hours of technical training each year, in addition to its existing MCLE requirements. Texas has nothing of this nature and doesn't offer MCLE credit for information technology training.

It's a sad day when Texas doesn't lead the way, especially when you consider that Texas is home to more world-class trial lawyers than the other forty-nine states put together--though 'course, it's not like a Texan to brag or nothin'.

About the Author

Craig Ball is a board-certified Texas trial lawyer, certified computer forensic examiner, law professor and electronic evidence expert He's dedicated his career to teaching the bench and bar about forensic technology and trial tactics. After decades trying lawsuits, Craig limits his practice to service as a court-appointed special master and consultant in computer forensics and e-discovery. A prolific contributor to educational programs worldwide--having delivered 2,000 presentations and papers--Craig's articles on forensic technology and electronic discovery frequently appear in the national media. For nine years, he wrote the award-winning column on computer forensics and e-discovery for American Lawyer Media called "Ball in your Court." Craig Ball has served as the Special Master or testifying expert on computer forensics and electronic discovery in some of the most challenging, front page cases in the U.S. (e.g., Enron, Madoff, In re: Seroquel, etc.).

EDUCATION

Rice University (B.A., 1979, triple major); University of Texas (J.D., with honors, 1982); Oregon State University (Computer Forensics certification, 2003); EnCase Intermediate Reporting and Analysis Course (Guidance Software 2004); WinHex Forensics Certification Course (X-Ways Software Technology 2005); Certified Data Recovery Specialist (Forensic Strategy Services 2009); Nuix Certified E-Discovery Specialist (2014); numerous other classes on computer forensics and electronic discovery.

SELECTED PROFESSIONAL ACTIVITIES

Law Offices of Craig D. Ball, P.C.; Licensed in Texas since 1982.
Board Certified in Personal Injury Trial Law by the Texas Board of Legal Specialization 1988-2017
Certified Computer Forensic Examiner, Oregon State University and NTI
Certified Computer Examiner (CCE), International Society of Forensic Computer Examiners
Certified Data Recovery Specialist
Certified E-Discovery Specialist (Nuix)
Faculty, University of Texas School of Law, Adjunct Professor teaching Electronic Discovery & Digital Evidence
Faculty and Founder, Georgetown University Law Center, E-Discovery Training Academy
Admitted to practice U.S. Court of Appeals, Fifth Circuit; U.S.D.C., Southern, Northern and Western Districts of Texas.
Board Member, Georgetown University Law Center Advanced E-Discovery Institute and E-Discovery Academy
Board Member, International Society of Forensic Computer Examiners *(agency certifying computer forensic examiners)*
Member, Sedona Conference WG1 on Electronic Document Retention and Production
Member, Maryland Committee on Federal E-Discovery Guidelines, 2014- (civil and criminal committees)
Special Master, Electronic Discovery, numerous federal and state tribunals
Instructor in Computer Forensics and Electronic Discovery, United States Department of Justice
Lecturer/Author on Electronic Discovery for Federal Judicial Center and Texas Office of the Attorney General
Instructor, HTCIA Annual 2010, 2011 Cybercrime Summit, 2006, 2007; SANS Instructor 2009, PFIC 2010, CEIC 2011, 2012
Special Prosecutor, Texas Commission for Lawyer Discipline, 1995-96
Council Member, Computer and Technology Section of the State Bar of Texas, 2003-date; Chair 2015-2016
Chairman: Technology Advisory Committee, State Bar of Texas, 2000-02
President, Houston Trial Lawyers Association (2000-01); President, Houston Trial Lawyers Foundation (2001-02)
Director, Texas Trial Lawyers Association (1995-2003); Chairman, Technology Task Force (1995-97)
Member, High Technology Crime Investigation Association and International Information Systems Forensics Assn.

Member, Texas State Bar College
Member, Continuing Legal Education Comm., 2000-04, Civil Pattern Jury Charge Comm., 1983-94, State Bar of Texas
Life Fellow, Texas and Houston Bar Foundations
Adjunct Professor, South Texas College of Law, 1983-88

Recipient of Lifetime Achievement Awards from the State Bar of Texas Computer and Technology Section (2006) and the Association of Certified E-Discovery Specialists (2016)
LTN Consultant of the Year, 2009

Selected Publications available at www.craigball.com