COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas

2016 January

TABLE OF CONTENTS

CLICK ON TITLE TO JUMP TO ARTICLE

President’s Message for Circuits January 2016

By Craig Ball

We live at the dawn of a golden age of evidence, ushered in by the monumental growth of data. When we access electronically stored information (ESI) and use digital devices, we generate and acquire vast volumes of electronic evidence. Never in the course of human history have we had so much probative evidence, and never has that evidence been so objective and precise. Lawyers, above all, should celebrate this boon; yet, many of our number bemoan electronic evidence because they’ve not yet awoken to its value.

As sources of digital evidence proliferate in the cloud, on mobile devices and tablets and within the burgeoning Internet of Things, the gap between competent and incompetent counsel grows. It’s become a crisis of competence, and we suffer most when standard setters refuse to define competence in any way that might exclude them. Vague pronouncements of a duty to stay abreast of “relevant technology” are noble, but don’t help lawyers know what they must know.

So, it is encouraging when California, with twice Texas’ number of lawyers, takes a strong, clear stand on what counsel must know about e-discovery. The State Bar of California Standing Committee on Professional Responsibility and Conduct issued a formal opinion in which the Committee sets out the level of skill and familiarity required when, acting alone or with assistance, counsel undertakes to represent a client in a matter implicating electronic discovery. Formal Opinion Interim No. 2015-193 (2015) states:

> Taken together generally, and under current technological standards, attorneys handling e-discovery should have the requisite level of familiarity and skill to, among other things, be able to perform (either by themselves or in association with competent co-counsel or expert consultants) the following:
>
> 1. initially assess e-discovery needs and issues, if any;
> 2. implement appropriate ESI preservation procedures, including the obligation to advise a client of the legal requirement to take actions to preserve evidence, like electronic information, potentially relevant to the issues raised in the litigation;
> 3. analyze and understand a client's ESI systems and storage;
> 4. identify custodians of relevant ESI;
> 5. perform appropriate searches;
> 6. collect responsive ESI in a manner that preserves the integrity of that ESI;

7. advise the client as to available options for collection and preservation of ESI;
8. engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan; and
9. produce responsive ESI in a recognized and appropriate manner.

Thus, California lawyers face a simple mandate when it comes to e-discovery, and one we Texas lawyers should take to heart: When it comes to handling cases with electronic evidence: Learn it, get help or get out.

Our mission at the Computer and Technology Section is to help you learn it, not just in e-discovery but everywhere law and technology intersect. Your membership supports that mission. Thank you.

Craig Ball, 2015-2016 Chair of the Computer and Technology Section, State Bar of Texas

COMPUTER AND
TECHNOLOGY
SECTION

RETURN TO TABLE OF CONTENTS

Letter from the Editors

By Elizabeth Rogers & Michael Curran

Dear Section Members:

As you may recall our Council Member, Jason Smith, was one of five finalists for the Innovator of the Year at the Awards Ceremony at International Legal Technology Association's 2015 Annual Conference. As our Bylaws state, the mission of the section is to "provide leadership on emerging issues at the intersection of law, science and technology; to promote sound policy and public understanding on such issues; and to enhance the professional development of its members." We were glad to support Jason and proud that his nomination gave international visibility to the State Bar of Texas' Computer and Technology Law Section and furthered our mission to provide leadership at the intersection of law, science and technology.

As we turn the corner into 2K16, we recognize several emerging issues at the intersection of law, science and technology that are relevant to our members. Specifically, many Texas attorneys will be impacted next year by matters involving:

- Technical innovations (advancements in programs, tools, apps, etc.)
- eDiscovery
- Privacy
- Cybersecurity and computer abuse
- Social media, and
- Professional responsibility, ethics, and technical competency

Please join us on our journey to bring leadership to Texas attorneys in these growing fields. You can contribute in many ways such as: sending us an article or blog to be highlighted in Section publications; joining us at our series of receptions statewide, for the purpose of not only networking, but also for the purpose of listening to your feedback of what you need from the Section; and, applying to join the Section Council for next year. We want you to participate. Happy 2K16! By working together, we can help your New Year to be one of the most efficient and prosperous to date.

Sincerely,

Elizabeth Rogers & Michael Curran

Wiretapping & Data Interception in Civil and Family Law Cases

By Hon. Emily Miskel

Civil and family law attorneys are increasingly confronted with situations where a client's information has been improperly accessed or where a client has obtained information improperly. The laws relating to interception of communications and electronic data are a confusing web of state and federal statutes, which can include harsh penalties and damages for clients. These laws can also create personal criminal and financial liability for lawyers.

There are three general categories of laws relating to interception of communications. At the federal level they are referred to as:

- the Wiretap Act (Title I of the Electronic Communications Privacy Act),
- the Stored Communications Act (Title II of the ECPA) , and
- the Computer Fraud and Abuse Act.

Texas has also adopted state versions of each law, with criminal offenses in the Texas Penal Code and civil causes of action in the Texas Civil Practice and Remedies Code.

Wiretap Act

The wiretap laws apply to communications that are intercepted *contemporaneously* with transmission. This can include in-person conversations, phone conversations, and even electronic communications, as long as the communication is intercepted at the time it is being transmitted. The wiretap laws have the most severe penalties, strict exclusionary rules, and highest statutory damages.

Use and Disclosure Liability – Under the Wiretap Act, it is also a violation to "use" or "disclose" any contents of a communication if you know or have reason to know that it was obtained through interception. Cases have held that attorneys' use of information obtained from a client's wiretapped recordings to prepare deposition questions, make settlement offers, report criminal activity, or even to play the recordings at trial are violations. These are separate, independent wiretap violations by the attorney, and the attorney is personally liable for $10,000 or more in statutory damages and possible criminal penalties.

RETURN TO TABLE OF CONTENTS

Exceptions – There are several exceptions to the Wiretap Act that permit recording. Under federal and Texas law, only one person in a communication need consent to a recording. In other words, a participant can record her communications. However, some states have all-party consent laws, and the law of the stricter state applies. It is safest to caution your clients not to record any conversation where a party may be outside Texas, without a disclosure that the communication may be recorded. A parent can give vicarious consent to the recording of a child's conversations if the parent has a good faith, objectively reasonable belief that the recording is necessary for the welfare of the child.

Stored Communications Act

The stored communications laws apply to communications that are intercepted while in electronic storage incident to transmission. Federal opinions conflict as to the interpretation of terms such as "temporary, intermediate storage" or "backup storage." For example, some courts have held that all webmail stored online is in electronic storage incident to transmission, while other courts have held that only unopened webmail is subject to an interception violation under the Stored Communications Act. In practice, proving a claim under stored communications laws can be complex because the success of the claim depends on technical fact issues as to how the electronic information was stored and sent.

Computer Fraud and Abuse Act

The Wiretap Act and Stored Communications Act would not generally apply to someone who obtained communications saved on the recipient's device. The Computer Fraud and Abuse Act (CFAA) and similar laws apply to circumstances where data is obtained locally from a person's computer or phone. These laws make it a violation to access a computer, network, or system without the effective consent of the owner, or to exceed authorization. Under the CFAA, "protected computer" includes any data processing device used in interstate commerce (i.e. any device that connects to the internet). Generally, proving a claim under the CFAA requires a minimum of $5,000 in damages, but that can include response costs, salaries of employees to repair the harms, lost profits, technical consultants, outside contractors, and more.

Violation of usage policies–Some federal courts have held that violating terms of service or a computer usage policy can be a violation of the CFAA. The 9th Circuit has taken a strong position against this broad application of the CFAA, but other circuits have enforced criminal penalties against, for example, employees who take an employer's electronic information.

Online Impersonation

Texas also has criminal and civil claims for online impersonation. It is a felony to impersonate someone by creating a web page or social media account, or sending messages through a website or social networking site. It is a misdemeanor to impersonate someone by sending email, instant messages, or text messages.

Originally published in the October 2015 issue of the Dallas Bar Association Headnotes.

About the Author

Emily Miskel is judge of the 470th district court in Collin Country. She can be reached at emily@emilymiskel.com.

Authentication of Cell Phone Text Messages

By Pierre Grosdidier

Parties seeking to admit cell phone text messages at trial face two authentication challenges. They must show that the documents they seek to admit into evidence are accurate copies of the original text messages, and they must show that the persons to whom they seek to ascribe the messages actually wrote them.[1] These issues are not just of interest to criminal defendants' counsel, as the largely-penal available case law suggests. Civil litigants may also seek to introduce text messages, or challenge their authenticity, in divorce or custody proceedings or in other civil litigation.[2]

Courts have uniformly held that existing rules of evidence are "generally 'adequate to the task'" of authenticating electronic information, despite its unique characteristics, and have declined to create new and special rules.[3] Under Texas Rule of Evidence 901(a), evidence authentication, *i.e.*, establishing that evidence is what its proponent claims it is, is a "condition precedent" to admissibility. Evidence that cannot be authenticated is not relevant and is inadmissible.[4]

Rule 901(a)'s authentication threshold is met "by evidence sufficient to support a finding that the matter in question is what its proponent claims."[5] This issue is a preliminary question of law for the judge under Texas Rule of Evidence 104(a). Only a threshold showing is necessary, the judge need not be personally convinced of the evidence's authenticity, and the rules of evidence do not apply to Rule 104 determinations. The trial court must simply decide "whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable

[1] There may be other evidentiary hurdles to admissibility, such as hearsay, but this article focuses on authentication. As to parties, text messages are not hearsay when they are the statements of a party against whom the messages are offered into evidence. *Aekins v. State*, No. 04-13-00064-CR, 2013 WL 5948188, at *6 (Tex. App.—San Antonio Nov. 6, 2013) (mem. op.), aff'd, 447 S.W.3d 270 (Tex. Crim. App. 2014). As to parties, then, they are admissible under the admission by party-opponent exception to the hearsay rule.

[2] *See, e.g., In re A.V.*, No. 04-15-00011-CV, 2015 WL 6535471 (Tex. App.—San Antonio Oct. 28, 2015, no pet. h.) (mem. op.) (child custody); *Howell v. Howell*, No. 13-10-00687, 2013 WL 784542 (Tex. App.—Corpus Christi Feb. 28, 2013, no pet.) (mem. op.) (divorce). Neither of these two cases challenged the authenticity of the text messages at issue.

[3] *Tienda v. State*, 358 S.W.3d 633, 638-39 (Tex. Crim. App. 2012).

[4] Tex. R. Evid. 402; *Tienda*, 358 S.W.3d at 638.

[5] Tex. R. Evid. 901(a).

jury determination that the" proffered evidence is authentic.[6] The jury ultimately decides the weight to give the admitted evidence.

The standard of admissibility under Rule 901(a) is rather liberal and can be met in a large number of ways, several of which are listed under Rule 901(b). Personal testimony of a knowledgeable witness is the most common and time-honored way of authenticating evidence.[7] Evidence can also be authenticated by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."[8] As the cases discussed in this article show, electronic evidence, including cell phone text messages, is most often authenticated through witness testimony and circumstantial evidence.[9]

A witness can authenticate photographs of cell phone text messages.

As noted, the first authentication hurdle is that of the text messages themselves, which reside on cell phones or other hand-held devices, from which they are not easily extracted and transcribed into print. One commentator has described this authentication issue as "the lesser one."[10] The messages can always be read into the record if they are not too long or too numerous. In *Montoya v. State*, an incriminating text message was read into the record, the cell phone was admitted into evidence, and the witness "pulled out [the] phone and pulled up the . . . text message for the attorneys to review."[11] In other cases, parties successfully introduced photographs of text messages. In *Butler v. State*, for example, the court allowed photographs of text messages taken on the victim's BlackBerry.[12] Two other courts did likewise in *Aekins* and in *Manuel v. State* with photographs taken on the victims' cell phones.[13] Photographs of text messages satisfy Rule 901's admissibility threshold provided that a witness can testify as to the photographs' authenticity.[14]

[6] *See generally, Tienda*, 358 S.W.3d at 637-38.

[7] Tex. R. Evid. 901(b)(1).

[8] *Id.* 901(b)(4).

[9] *See also*, Steven Goode, *The Admissibility of Electronic Evidence*, 29 Rev. Litig. 1, 9 (2009).

[10] *Id.* at 17.

[11] No. 05-10-01468-CR, 2012 WL 1059699, at *3 (Tex. App.—Dallas Mar. 30, 2012, no. pet.) (mem. op.).

[12] 459 S.W.3d 595, 599 (Tex. Crim. App. 2015).

[13] *Aekins*, No. 04-13-00064-CR, 2013 WL 5948188, at **5□6; 357 S.W.3d 66, 76 (Tex. App.—Tyler 2011, no pet.).

[14] In *Butler* and *Manuel*, the testifying witnesses (the victims) owned the photographed devices. In *Butler*, the State introduced the text messages via the victim's testimony. Likewise, in *Chavezcasarrubias v. State*, "the State elicited testimony from [the victim] that the text messages were a true and accurate

Of course, text messages can be also be extracted forensically from cell phones or can be requested from cell phone companies. Forensic extraction is costly, which is often not an insignificant consideration in family law cases. Cell phone companies will produce text messages to the cell phone's owner, but the process usually takes time. "Apps" now exist to export text messages on smart devices to computers, from where they can be conveniently printed.[15] In all these scenarios, the text message recipient must still testify as to authenticity. Unless the messages are numerous or lengthy, authenticated photographs seem like the simplest way to admit them into evidence.

Text message contents, context, and circumstances are key indicia of authenticity.

Ascribing text messages to their putative senders is not as straightforward. The Texas Court of Criminal Appeals held in *Tienda* that showing that a "text message emanates from a cell phone number assigned to the purported author" is not, without more, sufficient to establish the message's authenticity.[16] As the *Tienda* Court noted, "cell phones can be purloined" and someone other than the cell phone owner might have sent the messages. Authenticating cell phone text message authorship requires something more than establishing originating cell phone ownership. But as the following cases show, that "something more" is not very demanding under Rule 901(b)(4)'s liberal standard.

In *Butler*, the Court of Criminal Appeals reversed the Corpus Court of Appeals, which had reversed the defendant's conviction because of allegedly inadequately authenticated text messages.[17] The trial court had found Butler guilty of aggravated kidnapping of his girlfriend. A week before trial, Butler sent his then ex-girlfriend a series of emails threatening her and her family should she testify against him. Butler's foul-language-laced messages contained death threats and accused the victim of snitching to the police and betraying him. The victim testified that the messages came from a phone number that belonged to Butler, and that Butler also called her from that number between text messages "talking mess."

The Court of Criminal Appeals reasserted that the victim's knowledge and testimony that the phone number from which the text messages originated was Butler's was insufficient to establish Butler's authorship. But other evidence "bridged the gap and supplied the necessary

depiction of text messages between herself and Chavezcasarrubias." No. 02-14-00418-CR, 2015 WL 6081502, at *2 (Tex. App.—Fort Worth Oct. 15, 2015, no pet.) (mem. op.).

[15] *See*, e.g., www.imazing.com.

[16] *Tienda*, 358 S.W.3d at 642.

[17] *Butler*, 459 S.W.3d at 598.

predicate" for admissibility. In particular, the substance and context of the text messages accusing the victim of assisting authorities, and the threatening phone calls in-between text messages provided "additional circumstantial evidence" sufficient to authenticate the messages.

Similarly, in *Chavezcasarrubias*, the defendant was convicted of sexual crimes with an underage woman.[18] Chavezcasarrubias argued on appeal that text messages on the victim's cell phone were not "'sufficiently connected' to him" and were, therefore, improperly admitted into evidence. Both the trial court and the Court of Appeals disagreed. The witness had testified that she knew the cell phone number was Chavezcasarrubias' because she had previously communicated with him at that number by voice and via text messages, and the text messages contained information that only she and Chavezcasarrubias would have known. The Court of Appeals held that the victim's testimony sufficiently authenticated the text messages as Chavezcasarrubias'.

The defendant in *Gardner v. State* was convicted for armed robbery based on evidence that included text messages on his cell phone.[19] A witness positively identified Gardner as one of the robbers. One text message on Gardner's phone discussed practice-shooting a gun similar to the one used in the robbery. Another message sent an hour before the robbery stated that the sender was about to "hit a lick," urban argot for robbing someone.[20] The court held that this circumstantial evidence was sufficient to authenticate the messages as Gardner's.

Finally, in *Aekins*, the defendant challenged his sexual assault conviction based, in part, on an allegedly improperly authenticated text message.[21] The victim had received the message on her cell phone from an undisclosed phone number a few days before the assault. The message stated "Sorry if I offended u [sic]. Wil [sic] not do again," and it was signed "Soul." Three witnesses, including the victim and the defendant's wife, testified that "Soul" was Aekins's nickname. The victim also testified that she had received prior and similar messages from Aekins, and that this particular message appeared to have been sent in response to her complaining about Aekins's inappropriate advances. The court concluded that "[t]he events

[18] No. 02-14-00418-CR, 2015 WL 6081502, at *1.

[19] No. 02-14-00459-CR, 2015 WL 4652718, at *1 (Tex. App.—Fort Worth Aug. 6, 2015, pet. ref'd) (mem. op.).

[20] *Id.* ("' . . . hit a lick' . . . meant the person sending the text was about to commit a robbery."). According to urbandictionary.com, to "hit a lick" is "[t]o gain a s[***] load of mony [sic] in a short amount of time."

[21] No. 04-13-00064-CR, 2013 WL 5948188, at *6.

surrounding the message indicate circumstantially that [Aekins] was the author of the text message," and held that the latter was properly admitted into evidence.

Taken together, these cases show the relative ease with which cell phone text messages can be authenticated provided that the substance and context of the messages can be linked to the facts of the case.

About the Author

Pierre Grosdidier is an Attorney in Haynes and Boone, LLP's Litigation Department in Houston, Texas. His practice focuses on complex commercial litigation, especially lawsuits and arbitrations with strong technical elements. He has litigated cases involving construction, oil and gas, software copyright, Computer Fraud and Abuse Act, Stored Communications Act, and trade secret claims. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas and is a registered Texas P.E. (inactive).

RETURN TO TABLE OF CONTENTS

CLE is Terrible. It can be Better.

By Casey Flaherty

CLE is a horrible timesuck. Busy professionals endure endless droning about some boring topic while trying to concentrate on something else of immediate import. As both a panelist and guilty audience member, I've occupied many rooms where the collective sentiment shifts between apathy and anger at the colossal waste of time. Everyone sits there glued to their smartphone answering client emails or playing Angry Birds 2. As the leading researcher on how humans acquire new skills and information observes, lecture-style info dumps are a "great way to teach, but a terrible way to learn." Lectures are cost-effective but pedagogically unsound.

CLE is essential to the future of the profession. Even if law schools prepared lawyers for the world they were entering, they cannot prepare them for what that world will become. Change is just too rapid. The half-life of a learned skill used to be 30 years. That is, if you graduated law school in 1955, the world would have mostly passed you by 1985 if you had not updated your skill set. Today, the half-life of learned skill is 5 years. Most of the jobs the next generation will be doing do not exist yet. The good news for lawyers is that the fluid nature of the law long ago made us cognizant of the need for continuous learning. The bad news, of course, is that our current approach to CLE is terrible.

Not all CLE is terrible. For imparting big themes, generating interest, and starting a conversation, the traditional lecture can be fantastic if the speaker is good. Moreover, there are a fair number of dynamic, creative, and alternative approaches to CLE that get beyond the info-dump format. But most CLE is an endurance challenge now made easier by the ability to ignore an mp3 while you focus on clients' demands.

Time is a poor proxy for learning. Most lawyers would likely be horrified if admission to our profession merely required someone to sit in a law school class room for a prescribed period of time instead of passing a competence-based assessment. While we require the time, we also require a demonstration of actually having learned something because we know people are quite good at not paying attention. This approach is just not a barrier of entry for membership, it is also the premise of law school. Imagine if, instead of exams or projects, we gave full classroom credit for students who simply let videos play on their computer for the requisite length of time. Yet, that is precisely our approach with bar members. It's as if we believe that the transition to practice completely transforms the person and their attitude toward learning. We have decades of evidence to the contrary.

RETURN TO TABLE OF CONTENTS

Since time is a poor proxy for learning, I suggest that we measure learning directly. Computer-mediated competence-based assessments are not just a great way to verify knowledge/skill acquisition on the back end but a fantastic way to identify knowledge/skill acquisition on the front end. While it is a poor proxy for learning, time remains a valuable resource, and it should not be squandered on teaching people things they already know. One of the many problems with the lecture is that the lecturer is forced to assume the pre-existing knowledge level of the audience. The lecturer will always be wrong because the audience is a collection of individuals starting from vastly different baselines.

All of the foregoing is particularly apt when we are thinking about the skills required to work with specific technologies. Sitting through a demonstration of someone doing something new with a piece of software is not only boring, it is useless unless we have an almost immediate opportunity to apply what we see. Again, the lecture can be great for broad themes—e.g., what the software is capable of—but terrible for assimilating the actual skills—e.g., how to do it. For that, we need active learning, which is something that integrates extremely well with computer-mediated competence-based assessments.

You do not need to accept my heresy about competence-based CLE being superior to time-based CLE. We can pair the two. We can add optional competence-based components to our extant CLE offerings without any radical departure from the current arrangement. I'll provide concrete examples of what that might look like in my next column.

About the Author

Casey Flaherty is a lawyer, consultant, writer, and speaker based in Austin, TX. Casey is a former in-house counsel and the creator of the Legal Technology Assessment, an integrated technology and training platform. Follow Casey on LinkedIn and on Twitter, @DCaseyF.

Databases in Discovery

By Craig Ball

I loathe the practice of law from forms, but bow to its power. Lawyers love forms; so, to get lawyers to use more efficient and precise prose in their discovery requests, we can't just harangue them to do it; we've "got to put the hay down where the goats can get it." To that end, here is some language to consider when seeking information about databases and when serving notice of the deposition of corporate designees (*e.g.*, per Rule 30(b)(6) in Federal civil practice or Rule 199(b)(1) of the Texas Rules of Civil Procedure):

For each database or system that holds potentially responsive information, we seek the following information to prepare to question the designated person(s) who, with reasonable particularity, can testify on your behalf about information known to or reasonably available to you concerning:

1. The standard reporting capabilities of the database or system, including the nature, purpose, structure, appearance, format and electronic searchability of the information conveyed within each standard report (or template) that can be generated by the database or system or by any overlay reporting application;
2. The enhanced reporting capabilities of the database or system, including the nature, purpose structure, appearance, format and electronic searchability of the information conveyed within each enhanced or custom report (or template) that can be generated by the database or system or by any overlay reporting application;
3. The flat file and structured export capabilities of each database or system, particularly the ability to export to fielded/delimited or structured formats in a manner that faithfully reflects the content, integrity and functionality of the source data;
4. Other export and reporting capabilities of each database or system (including any overlay reporting application) and how they may or may not be employed to faithfully reflect the content, integrity and functionality of the source data for use in this litigation;
5. The structure of the database or system to the extent necessary to identify data within potentially responsive fields, records and entities, including field and table names, definitions, constraints and relationships, as well as field codes and field code/value translation or lookup tables.

6. The query language, syntax, capabilities and constraints of the database or system (including any overlay reporting application) as they may bear on the ability to identify, extract and export potentially responsive data from each database or system;
7. The user experience and interface, including datasets, functionality and options available for use by persons involved with the **PROVIDE APPROPRIATE LANGUAGE RE THE ACTIVITIES PERTINENT TO THE MATTERS MADE THE BASIS OF THE SUIT**;
8. The operational history of the database or system to the extent that it may bear on the content, integrity, accuracy, currency or completeness of potentially responsive data;
9. The nature, location and content of any training, user or administrator manuals or guides that address the manner in which the database or system has been administered, queried or its contents reviewed by persons involved with the **PROVIDE APPROPRIATE LANGUAGE RE THE ACTIVITIES PERTINENT TO THE MATTERS MADE THE BASIS OF THE SUIT**;
10. The nature, location and contents of any schema, schema documentation (such as an entity relationship diagram or data dictionary) or the like for any database or system that may reasonably be expected to contain information relating to the **PROVIDE APPROPRIATE LANGUAGE RE THE ACTIVITIES PERTINENT TO THE MATTERS MADE THE BASIS OF THE SUIT**;
11. The capacity and use of any database or system to log reports or exports generated by, or queries run against, the database or system where such reports, exports or queries may bear on the **PROVIDE APPROPRIATE LANGUAGE RE THE ACTIVITIES PERTINENT TO THE MATTERS MADE THE BASIS OF THE SUIT**;
12. The identity and roles of current or former employees or contractors serving as database or system administrators for databases or systems that may reasonably be expected to contain (or have contained) information relating to the **PROVIDE APPROPRIATE LANGUAGE RE THE ACTIVITIES PERTINENT TO THE MATTERS MADE THE BASIS OF THE SUIT**; and
13. The cost, burden, complexity, facility and ease with which the information within databases and systems holding potentially responsive data relating to the **PROVIDE APPROPRIATE LANGUAGE RE THE ACTIVITIES PERTINENT TO THE MATTERS MADE THE BASIS OF THE SUIT**; may be identified, preserved, searched, extracted and produced in a manner that faithfully reflects the content, integrity and functionality of the source data.

Yes, this is the dread "discovery about discovery;" but, it's a necessary precursor to devising query and production strategies for databases. If you don't know what the database holds or the ways in which relevant and responsive data can be extracted, you are at the mercy of opponents who will give you data in unusable forms or give you nothing at all.

Remember, these are not magic words. I just made them up, and there's plenty of room for improvement. If you borrow this language, please take time to understand it, and particularly strive to know *why* you are asking for what you demand. Supplying the information requires effort that should be expended in support of a genuine and articulable need for the information. If you don't need the information or know what you plan to do with it, don't ask for it.

These few questions were geared to the feasibility of extracting data from databases so that it stays utile and complete. Enterprise databases support a raft of standardized reporting capabilities: "screens" or "reports" run to support routine business processes and decision making. An insurance carrier may call a particular report the "Claims File;" but, it is not a discrete "file" at all. It's a predefined template or report that presents a collection of data extracted from the database in a consistent way. Lots of what we think of as sites or documents are really reports from databases. Your Facebook page? It's a report. Your e-mail from Microsoft Outlook? Also a report.

In addition to supplying a range of standard reports, enterprise databases can be queried using enhanced reporting capabilities ("custom reports") and using overlay reporting tools-commercial software "sold separately" and able to interrogate the database in order to produce specialized reporting or support data analytics. A simple example is presentation software that generates handsome charts and graphics based on data in the database. The presentation software didn't come with the database. It's something they bought (or built) to "bolt on" for enhanced/overlay reporting.

Databases are constructed to enforce specified field property requirements or "constraints." These may include:

1. **Field size**: limiting the number of characters that can populate the field or permitting a variable length entry for memos;
2. **Data type**: text, currency, integer numbers, date/time, e-mail address and masks for phone numbers, Social security numbers, Zip codes, etc.;

3. **Unique fields**: Primary keys must be unique. You typically wouldn't want to assign the same case number to different matters or two Social Security numbers to the same person;
4. **Group or member lists**: Often fields may only be populated with data from a limited group of options (e.g., U.S. states, salutations, departments and account numbers);
5. **Validation rules**: To promote data integrity, you may want to limit the range of values ascribed to a field to only those that makes sense. A field for a person's age shouldn't accept negative values or (so far) values in excess of 125. A time field should not accept "25:00pm" and a date field designed for use by Americans should guard against European date notation. Credit card numbers must conform to specific rules, as must Zip codes and phone numbers; and
6. **Required data**: The absence of certain information may destroy the utility of the record, so certain fields are made mandatory (e.g., a car rental database may require input of a valid driver's license number).

Databases are queried using a "query language." Users needn't dirty their hands with query languages because queries are often executed "under the hood" by the use of those aforementioned standardized screens, reports and templates. Think of these as pre-programmed, pushbutton queries. There is usually more (and often much more) that can be gleaned from a database than what the standardized reports supply, and some of this goes to the integrity of the data itself. In that case, understanding the query language is key to fashioning a query that extracts what you need to know, both *within* the data and *about* the data.

As importantly as learning what the database can produce is understanding what the database does or does not display to end users. These are the *user experience* (UX) and *user interface* (UI). Screen shots may be worth a thousand words when it comes to understanding what the user saw or what the user might have done to pursue further intelligence.

Enterprise and commercial databases tend to be big and expensive. Accordingly, most are well documented in manuals designed for administrators and end users. When a producing party objects that running a query is burdensome, the manuals may make clear that what you seek is no big deal to obtain.

In simplest terms, a database's schema is how it works. It may be the system's *logical schema*, detailing how the database is designed in terms of its table structures, attributes, fields,

RETURN TO TABLE OF CONTENTS

relationships, joins and views. Or, it could be its *physical schema*, setting out the hardware and software implementation of the database on machines, storage devices and networks. The schema of a database is rarely a trade secret or proprietary data; although, you may hear that objection raised to frustrate discovery. The schema is more like a database map, typically supplied as a table or diagram.

One feature that sets databases apart from many others forms of ESI is the critical importance of the fielding of data. **Preserving the fielded character of data is essential to preserving its utility and searchability.** I wrote about this recently in "*The Virtues of Fielding*" (Circuits, Vol 3: Summer 2015). "Fielding data" means that information is stored in locations dedicated to holding just that information. Fielding data serves to separate and identify information so you can search, sort and cull using just that information. It's a capability we take for granted in databases but that is often crippled or eradicated when data is produced in e-discovery. **Be sure that you consider the form of production, and insure that the fielded character of the data produced will not be lost, whether supplied as a standard report or as a delimited export.**

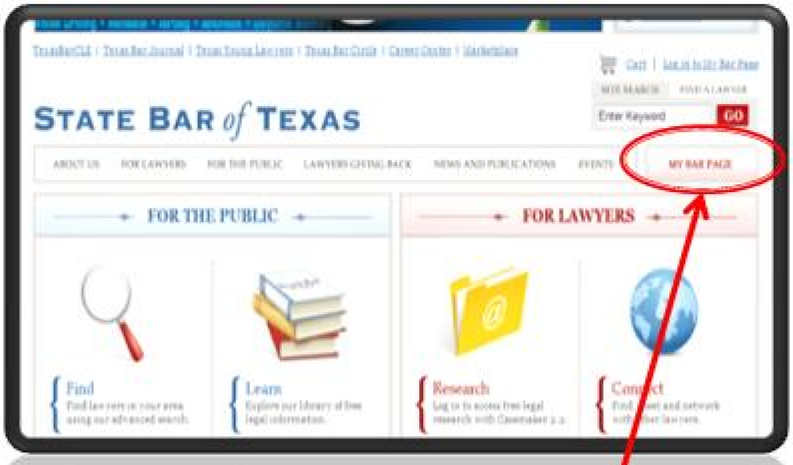
Seeking discovery from databases is a key capability in modern litigation, and it's not easy for the technically challenged (although it's probably a whole lot easier than your opponent claims). Getting the proper data in usable forms demands careful thought, tenacity and more-than-a-little homework. Still, anyone can do it, alone with a modicum of effort, or aided by a little expert assistance.

About the Author

Craig Ball of Austin is a Board-certified trial lawyer who limits his practice to service as a court-appointed Special Master and consultant in computer forensics and electronic discovery. A founder of the Georgetown University Law Center E-Discovery Training Academy, Craig serves on the Academy's faculty and also teaches Electronic Discovery and Digital Evidence at the University of Texas School of Law. For nine years, Craig penned the award-winning column on electronic discovery for American Lawyer Media and now writes for several national news outlets. Craig has published and presented on forensic technology more than 1,700 times, all over the world. For his articles on electronic discovery and computer forensics, please visit craigball.com or ballinyourcourt.com.

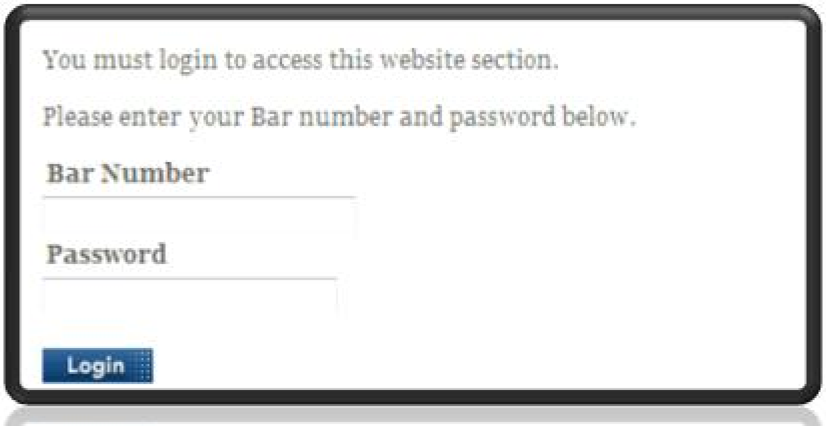
How to Join the State Bar of Texas Computer & Technology Section

Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.



Step 1

Go to Texasbar.com and click on "My Bar Page"



You must login to access this website section.

Please enter your Bar number and password below.

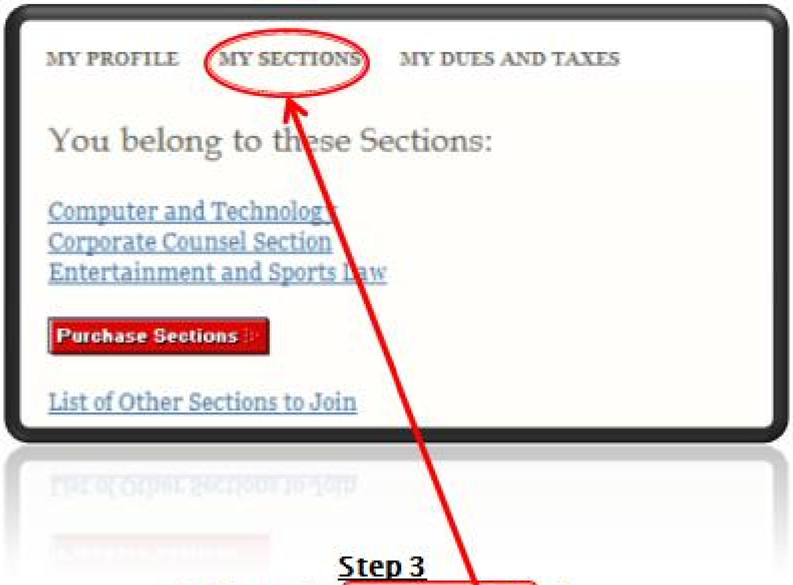
Bar Number

Password

Step 2

Login using your bar number and password

(this will be the same information you'll use to login to the Section website)



You belong to these Sections:

Computer and Technology
Corporate Counsel Section
Entertainment and Sports Law

List of Other Sections to Join

Step 3
Click on the "My Sections" tab

If you see "Computer and Technology", congratulations, you're already a member.

If not, click the "Purchase Sections" button and follow the instructions to add the Computer and Technology Section. **Please note: It may take several days for the State Bar to process your section membership and update our system.**

You can also complete this form and mail or fax it in.

State Bar of Texas Computer & Technology Section Council

Officers

Craig Ball – Austin – Chair
Eric Griffin – Dallas – Chair-Elect
Shannon Warren – Houston – Treasurer
Michael Curran – Austin – Secretary
Joseph Jacobson – Dallas – Past Chair

Term Expiring 2016

Sammy Ford IV – Houston
John Browning – Dallas
Reginald Hirsch – Houston

Term Expiring 2017

Elizabeth Rogers– Austin
Shawn Tuma – Dallas
Bert Jennings – Houston

Term Expiring 2018

Megan Carter – Dallas
Pierre Grosdidier – Houston
David Coker – Dallas
Laura Leonetti – Houston

Chairs of the Computer & Technology Section

2015-2016: Craig Ball
2014-2015: Joseph Jacobson
2013-2014: Antony P. Ng
2012-2013: Thomas Jason Smith
2011-2012: Ralph H. Brock
2010-2011: Grant Matthew Scheiner
2009-2010: Josiah Q. Hamilton
2008-2009: Ronald Lyle Chichester
2007-2008: Mark Ilan Unger
2006-2007: Michael David Peck
2005-2006: Robert A. Ray
2004-2005: James E. Hambleton
2003-2004: Jason Scott Coomer
2002-2003: Curt B. Henderson
2001-2002: Clint Foster Sare
2000-2001: Lisa Lynn Meyerhoff
1999-2000: Patrick D. Mahoney
1998-1999: Tamara L. Kurtz
1997-1998: William L. Lafuze
1996-1997: William Bates Roberts
1995-1996: Al Harrison
1994-1995: Herbert J. Hammond
1993-1994: Robert D. Kimball
1992-1993: Raymond T. Nimmer
1991-1992: Peter S. Vogel
1990-1991: Peter S. Vogel

RETURN TO TABLE OF CONTENTS