Contents

Letter from the Chair

By Shannon Warren

As a large section, C&T purposely set objectives for education in 2016-2017. A tentative idea transformed into a quick plan of implementation to bring all Bar members short and focused videos of technology-related topics. After much discussion, past Chair Michael Peck spearheaded the planning and organization to implement the Council's idea. On May 9, several Council members stopped in at the Texas Bar CLE offices and recorded fifteen minute sessions that will be available at no charge to Bar members. Some of the topics addressed include cloud computing and law practice management, data privacy and cybersecurity, eDiscovery and document review, informed consent and engagement agreements. Whenever possible, ethics was woven in to the presentation, which makes these sessions one of a kind. Seventeen sessions in less than seven hours on the first recording is impressive and proudly represents the C&T. The professionalism and assistance from TexasBarCLE simply cannot be described, and my thanks to them is one of many echoed throughout the Council. Future recording sessions are planned, and with a measured success, we hope to launch this idea to other associations and provide attorneys struggling with every day technology issues confidentially resolve them. To say that I am absurdly proud of this accomplishment is an understatement.

In support of its focus on education, the Council attended Legaltech 2017 in February, which featured over 350 speakers, including two of the C&T Council members, Judge Xavier Rodriguez of the Western District of Texas and Craig Ball, an internationally known Special Master. The Council met to conduct quarterly business and again for a celebratory dinner before attending the closing sessions of the conference. As another testament to the skillset of the Section, Craig Ball was interviewed by Nina Totenberg as a Thought Leader during the event.

As a perk of membership, C&T members can access the section's mobile app, a comprehensive law library at one's fingertips. With a few clicks, a user has access to current rules and codes with links to cases. Section members also receive complimentary membership to the International Legal Technology Association, which boasts more than 20,000 members with access to star-quality professionals, programming, and publications, often leading the legal tech world. Circuits, a newsletter written by members of the section, offers articles on trending technology issues and practical tips for the practicing legal profession.

As my year as Chair comes to a close, my appreciation for the efforts of members of the Council, C&T Section, State Bar and its staff, TexasBarCLE, and the many others that have helped keep the glue together for this Section. It has been my pleasure to serve and while I look forward to staying involved, I look forward to seeing the next idea this great Section implements.

COMPUTER AND
TECHNOLOGY
SECTION

Letter from the Editors

By Elizabeth Rogers and Antony P. Ng

In this quarter's issue of *Circuits*, the articles span the spectrum of providing practical tips for solo practitioners to providing a summary of the most recent regulations for the everyday cybersecurity security counselor. Our goal is to serve the interests and scholarly education of all members of the computer and technology section from contributors who are experts in their particular subject matter.

Many people are familiar with software applications, such as DropBox, for sharing files that are too large for standard email attachments. But many of those software applications do not provide adequate data security; consequently, they are not generally suitable for file sharing between attorneys and their clients due to security reasons. Ron Chichester is one of the leaders of our Section in the field of practical advice for solo practitioners. In his article, Chichester talks about some file sharing applications that do provide adequate security.

Meanwhile, state governments around the country are studying the economic havoc that sloppy cybersecurity practices can create for their economy. New York has gone beyond merely studying the impact and has become the first state to actually implement cybersecurity regulations, through the New York Department of Financial Services, meant to protect its citizens (and citizens around the world for that matter) from the ruin that a cybersecurity event in the financial services industry may cause. Shawn Tuma, a cybersecurity legal specialist, explains some critical steps that vendors of financial institutions, banks and insurance agencies must take in order to comply with the newly enacted cybersecurity laws, regardless of whether or not the vendors actually do business in New York.

Meanwhile, have you been wondering whether your sign-off in an email is a binding 'signature' for purposes of contract law? Texas appellate courts currently differ on just what effect your signature block might have. Another article in this issue, submitted by our own "Professor" John Browning, surveys the state of Texas law on this issue, examining recent case law on how email signature blocks can satisfy the Uniform Electronic Transactions Act and the Statute of Frauds. And, finally, it is always an intellectual treat to hear from Craig Ball, a lawyer's lawyer who shares some of his most recent e-discovery strategies for both requesting and producing parties.

As always, we hope that you enjoy the content of the current edition. We also encourage you to help us to make *Circuits*, a well-rounded publication for lawyers with interests in technology, and you can assist us by contributing your own articles and/or providing feedback and suggestions to Elizabeth Rogers at rogersel@gtlaw.com or Antony P. Ng at ng@russellnglaw.com.

Safe Alternatives to Box and Dropbox

By Ron Chichester

Ways to exchange large files (or numbers of files) with your client, and keep your law license.

Purpose

This article is one of a series that caters to small law offices in Texas (e.g., five or fewer attorneys). The articles will cover topics involving technology that small law firms need on an occasional basis , but not frequently enough to warrant the purchase of a license or subscription. In other words, something on the cheap for occasional use, and also something that is less likely to cause a violation of the Disciplinary Rules.

Some History

Several members of the Computer & Technology Section attended the Legal Tech New York conference that was held in late January, 2017. As with many large conferences about legal technology, the participating vendors predominately catered to the needs of large law firms. Indeed, according to the measure of the conference organizers, small law firms had up to *fifty* attorneys. of the many dozens of vendors that participated, only three had something of merit for small law firms in Texas. One of those vendors was a company called TitanFile. As the company name suggests, it enables attorneys to transfer large files to their clients without the use of DropBox or Box. TitanFile has a subscription service that starts at the cost of $15 per month, a price that is comparable to Box (minimum of three users at $5/month). DropBox has a free option, but the space for that option is capped at 2 GB.

Problems with the Paid Services

One of the challenges of using Box and DropBox is the perceived lack of reliable information security. As a consequence of the security concerns, the Texas Disciplinary Rules of Professional Conduct are implicated. Rule 1.05(b) (1) (ii), regarding Client Confidences might be violated by attorneys who upload client confidences to a cloud service like Box or DropBox because once the files are uploaded to those services, the client confidences are outside the possession or (complete) control of the attorney. It should be said at this point that the Bar has not expressly stated that those services run afoul of 1.05, but attorneys have refrained from using Box or DropBox for client information precisely because the attorney cannot completely control who has access to that information, how or where the information is backed up, and who has the keys to any encryption used (or not).

Is There a Less Expensive Alternative?

The answer is: *Yes!* Does that less expensive alternative require the purchase of a software license? *No*. Does the less expensive alternative require a short-term subscription? *No*.

Enter OwnCloud.

OwnCloud is an open source alternative for Box and DropBox that includes more options than just file storage and file sharing. With OwnCloud, you can sync calendars, contacts, mail and more.

As the name suggests, you own your instances of OwnCloud. All that you need is a standard web browser *and* a machine to run it that is accessible via the Internet. For some attorneys, however, the requirement of an Internet-accessible machine may be a show stopper. However, don't let that deter you because...

Enter DigitalOcean.

DigitalOcean is a service that hosts virtual machines accessible via the Internet. DigitalOcean offers "Droplets" which are pre-configured machines that you create (on demand), use, and then destroy. You pay only for as long as the machine is in existence.

Does DigitalOcean have a pre-configured droplet for OwnCloud? *Yes!* This means that you can install and deploy OwnCloud on an Internet-accessible machine in about 55 seconds.

The primary advantage for using DigitalOcean is that the attorney has complete control of the OwnCloud virtual machine. You create a droplet. Tell OwnCloud who can access it (e.g., your client), and transfer the data with your client. When you're finished, simply delete the droplet. Note that once a droplet has been deleted, no one can get it back. That data is gone forever. However, because the droplet can be deleted, clients are assured that the data on that server is permanently erased.

It gets better. Because OwnCloud is open source software, other companies have adopted it for the same reasons that DigitalOcean has.

Enter Amazon Web Services.

Amazon Web Services also has pre-configured OwnCloud virtual machines that can be created quickly and easily. Depending on what you're doing, Amazon's pricing may be more attractive than DigitalOcean's.

Conclusion

Texas attorneys have a low-cost option for transferring large numbers of (or just large) files with their clients in a way that doesn't require the relinquishment of control over the client's information to a third party. Once the transfer is concluded, any information still on the Cloud can be destroyed reliably and permanently. Moreover, the attorney need incur (minimal) costs for only as long as necessary, saving the attorney money and minimizing potential exposure. The services can be had on demand, with no need to incur subscription fees.

About the Author

Ron Chichester practices in the Houston area and specializes in technology-related law, particularly intellectual property, electronic discovery, cybersecurity/cybercrimes/cybertorts, electronic commerce and technology licensing. He is a past chair of the Computer & Technology Section of the Texas Bar, and is currently the Immediate Past Chair of the Business Law Section. He is also an Adjunct Professor at the University of Houston where he teaches classes on Digital Transactions (an intellectual property/e-commerce survey course) and Computer Crime. Ron holds a B.S. and an M.S. (both in aerospace engineering) from the University of Michigan and a J.D. from the University of Houston Law Center. For more information, please visit http://www.texascomputerlaw.com

Getting to Grips with New York's Cybersecurity Compliance Rules

By Shawn E. Tuma

Boards of directors must actively oversee cybersecurity, with the chairman or senior officer certifying compliance, according to a new regulation in New York that will impact companies worldwide.

The cybersecurity threat to companies is ubiquitous and no industry or region is immune. Recognizing the seriousness of this risk, the New York Department of Financial Services (NYDFS) developed proposed Cybersecurity Requirements for Financial Services Companies (the 'cybersecurity regulations') that became effective on 1 March 2017.

The new law, a first of its kind, contains multiple requirements for direct board involvement in cybersecurity of companies regulated by the NYDFS (covered entities) in addition to those companies that are third-party service providers for covered entities. Specifically, the board is required to take responsibility for the overall cybersecurity program, review and approve its company's cybersecurity policy, obtain cybersecurity reports from the chief information security officer at least annually and either the board's chairman or a senior officer must sign a written certification of compliance with the regulations on an annual basis. Those who sign off on these certifications, and their companies, must take these seriously as the NYDFS has very broad authority to investigate both civil and criminal matters that fall within its scope of authority.

Overview of the cybersecurity regulations

The NYDFS's goal was to promote the protection of customer information and the information technology systems of businesses by establishing certain minimum standards for business to adhere to but not be overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. This is directed at protecting companies' information systems and non-public information, both of which are specifically defined.

The cybersecurity regulations do this by focusing on three key goals that cybersecurity experts have regularly identified as being crucial to improving businesses' cybersecurity posture. They provide an outline of essential minimum standards for businesses to implement, designate who in the organization should be appointed to lead the process and mandate top down buy-in to the process by management and the board of directors. In general, they require three key things:

1. Each company must assess its specific risk profile and design a program that addresses its risks in a robust fashion, develop policies, procedures and training for personnel to address such risks and respond to incidents
2. Each company must designate a qualified individual to serve as its chief information security officer, responsible for overseeing and implementing its cybersecurity program, reporting on its cybersecurity program and notifying the NYDFS of any material incidents
3. Each company's senior management must be responsible for its cybersecurity program and file an annual certification, confirming compliance with the cybersecurity regulations or certify that it meets the criteria to be exempt

The NYDFS designed the regulations to establish minimum standards for companies while not being overly prescriptive so that cybersecurity can remain flexible to match the relevant risks and keep pace with technological advances. These general objectives are accomplished through specific requirements designed to improve companies' cybersecurity through a combination of technological policy-driven measures.

Though this list is not exhaustive, here are some of the specific requirements that are addressed: data governance and classification, access controls and identity management, systems and network security, penetration testing and vulnerability assessments, audit trail systems, access privileges, application security, adequate cybersecurity professionals, multi-factor authentication, data retention policies, training and monitoring of authorized users and encryption of non-public information, both in transit and at rest.

Global impact of cybersecurity regulations

Businesses in all industries across the US and abroad will likely be impacted by the regulations, despite being a product of New York law directed at businesses regulated by the Department of Financial Services. There are two reasons for this. First, the vast breadth of businesses that fall within the NYDFS' authority includes financial services-related businesses in New York, including banks, insurance companies and various other financial institutions. Second, the cybersecurity regulations require that such businesses contractually obligate third parties that they do business with to comply with provisions of the cybersecurity regulations. Because so many companies do business with companies related to the New York financial services industry, the reach will be global.

"THE REACH OF THE NYDFS CYBERSECURITY REGULATIONS WILL EXPAND FAR BEYOND THE COMPANIES THAT IT DIRECTLY REGULATES TO INCLUDE, TO A CERTAIN DEGREE, THOSE COMPANIES THAT DO BUSINESS WITH THEM"

The mission of the NYDFS is "[to] reform the regulation of financial services in New York to keep pace with the rapid and dynamic evolution of these industries, to guard against financial crises and to protect consumers and markets from fraud". It does this through its authority to take any actions necessary to:

- Foster the growth of the financial industry in New York and spur state economic development through judicious regulation and vigilant supervision
- Ensure the continued solvency, safety, soundness and prudent conduct of the providers of financial products and services
- Ensure fair, timely and equitable fulfilment of the financial obligations of such providers
- Protect users of financial products and services from financially impaired or insolvent providers of such services
- Encourage high standards of honesty, transparency, fair business practices and public responsibility
- Eliminate financial fraud, other criminal abuse and unethical conduct in the industry
- Educate and protect users of financial products and services and ensure that users are provided with timely and understandable information to make responsible decisions about financial products and services

By requiring adequate cybersecurity safeguards for companies that play a role in the financial services industry, the NYDFS is fulfilling multiple aspects of its policy objectives.

Impact on companies that are directly regulated by the NYDFS

The NYDFS cybersecurity regulations apply to what they define as covered entities. "Covered entity means any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law. Put simply, a covered entity is any entity regulated by the NYDFS."

The NYDFS' reach is expansive in looking only at the companies that it regulates directly. As expected, this includes banks and trust companies, credit unions, foreign bank branches, licensed lenders, health insurers, life insurance companies, property and casualty insurance companies and savings and loan associations. There are many more companies that may not be so easily expected:

- Bail bond agents
- Budget planners
- Charitable foundations
- Cheque cashers
- Holding companies
- Investment companies
- Money transmitters
- Service contract providers ("[Any] person or entity who sells or administers a service contract and who is contractually obligated to provide service under the service contract").

The last one – service contract providers – is extremely expansive and has the potential to pull many companies within the scope of being directly regulated by the NYDFS without those companies fully appreciating the implications.

Covered entities that meet the following criteria are exempted from some of the requirements of the regulations, although most are still required:

- Have fewer than 10 employees, including any independent contractors
- Have less than $5million in gross revenue in each of the last three fiscal years
- Have less than $10million in year-end assets – these entities are exempted from some, but not all, requirements of the regulations

Impact on companies that are indirectly regulated – third-party service providers to covered entities

The reach of the NYDFS' cybersecurity regulations will expand far beyond the companies that it directly regulates to include, to a certain degree, those companies that do business with them. Section 500.11 of the Regulations specifically addresses the cybersecurity of such third parties and requires covered entities to obtain satisfactory assurances that those they do business with have adequate cybersecurity safeguards.

When thinking about one of the objectives of the cybersecurity regulations, as well as most other cybersecurity and privacy policies and frameworks, it is to protect the confidentiality, integrity and accessibility of the information and computer systems. This requires protecting the information always, wherever it may be and with whoever may have possession of it. This also requires having protections in place for all systems that will interact with the covered entity's network. By implementing these third-party requirements, the NYDFS is trying to ensure that a covered entity's information is protected the same way by third parties who may receive the information is it is when it is in the custody of the covered entity. This is the same method that is used under HIPAA (Health Insurance Portability and Accountability Act of 1996) for protecting health information that is transferred from a covered entity under that framework to a business associate. Essentially, this means that third-party business partners are becoming business associates.

The cybersecurity regulations decree that a covered entity's chief information security officer requires the third-party service provider to maintain a cybersecurity program that meets the requirements of the cybersecurity regulations. It further requires the covered entity to implement written policies and procedures designed to ensure the security of information systems and non-public information that are accessible to, or held by, third parties doing business with the covered entity. The regulations make it a requirement for their contracts via contractual provisions and/or guidelines addressing cybersecurity. They do not include an exception from some of the requirements for smaller third-party service providers, like those for smaller covered entities.

What do the cybersecurity regulations mean for all companies?

Many businesses already have relatively mature cybersecurity programs in place and for those businesses the cybersecurity regulations may not have too great of an impact. Many businesses, however, do not have such programs and are lost in the wilderness of confusion in determining what they should be doing and how they should be doing it. For those businesses, the regulations should provide a basic guide to help them develop and implement an appropriate cybersecurity program.

The regulations were released on 13 September 2016 in a non-finalized form, subject to public comment, with an initial effective date of 1 January 2017. Given the substantial feedback that was generated, they were revised significantly and re-released on 28 December 2016. Businesses should anticipate that they will be codified in substantially similar form as they are now and prepare accordingly.

The effective date was delayed to 1 March 2017, but businesses that are directly regulated by the NYDFS must begin preparing now so that they will comply with the regulations by the time the law goes into effect. Non-NYDFS regulated businesses that do business with regulated entities and have access to or hold non-public information of covered entities or their information systems (third-party service providers) will be subject to certain mandatory requirements to ensure the covered entities' non-public information and information systems remain adequately protected. Covered entities will be required to develop preferred contract provisions for such third-party service providers that permit the covered entity to assess their cybersecurity posture, require they implement specific cybersecurity measures to protect the non-public information and information systems, establish notification and remediation requirements in case of a cybersecurity incident, and allocate who pays the costs for such an incident.

The substantive requirements of these contracts will have little room for negotiation because they are being pushed down by the requirements of the law. Moreover, because these contractual protections are to protect the non-public information and information systems, they must flow along with such data and systems access and be pushed down to other contractors and sub-contractors who have such access.

Businesses that may find themselves in this situation need to have an adequate understanding of these requirements so that they can differentiate between those things the covered entity must do vis-à-vis those things it wishes to do when negotiating these contracts. They also need to begin preparing so that they will have appropriate cybersecurity measures in place to satisfy the requirements of the cybersecurity regulations that are passed along to them via contract and that they must then pass along to those with whom they do business where the covered entity's sensitive personal information is being shared.

[Previously published on ethicalboardroom.com]

About the Author:

Shawn Tuma (@shawnetuma) is a cybersecurity lawyer business leaders trust to help solve problems with cutting-edge issues involving cybersecurity, data privacy, computer fraud and intellectual property law. Shawn is a frequent author and speaker on these issues and has used social media to help build his practice. He is a partner at Scheef & Stone, LLP, and a full service commercial law firm in Texas that represents businesses of all sizes throughout the United States and, through its Mackrell International network, throughout the world.

No Ink, No Problems? Validity of Email Signatures as Contracts

By John G. Browning

Let's face it: in today's Digital Age more and more businesses are conducting their transactions electronically. By one 2015 estimate, over 205 billion emails are sent and received every day.[1] Congress and nearly all states have facilitated the spread of electronic commerce through laws governing the validity of electronically signed documents and electronic transactions. On the federal level, we have the Electronic Signatures in Global and National Commerce Act (often referred to as the "E-Sign Act"), enacted in 2000. At the state level, there is the Uniform Electronic Transaction Act, or UETA, which makes the E-Sign Act applicable to electronic signatures and electronic transactions governed by state law. Both the federal statute and its state counterparts treat electronic transactions and signatures the same as more traditional ink and paper documents and transactions. But while Texas – which adopted the UETA in 2001 – has generally followed this trend, a recent split of authorities among Texas appellate courts has made the question of whether the signature line in an email actually constitutes a "signature" (for the purpose of satisfying the Statute of Frauds) a bit murkier.

First let's provide some background. Texas' Uniform Electronic Transactions Act, found in Section 322.001-.022 of Texas Business & Commerce Code, states that, "[i]f a law requires a record to be in writing, an electronic record satisfies the law."[2] It further holds that "[i]f a law requires a signature, an electronic signature satisfies the law."[3] And just what is an "electronic signature" according to the UETA? It is "an electronic sound, symbol, or process attached to or logically associated with a record or executed or adopted by a person with the intent to sign the record."[4] More specifically, an electronic signature is "attributable to a person if it was the act of the person,"[5] the effect of which can be determined from "the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law."[6]

[1] "Email Statistics Report, 2015-2019," The Radicati Group (www.radicati.com). The report further estimated that this figure would grow at an average annual rate of 3% over the next four years, reaching over 246 billion per day by the end of 2019.

[2] Tex. Bus. & Com. Code § 322.007 (c).

[3] *Id*. at (d).

[4] Tex. Bus. & Com. Code § 322.007 (8).

[5] *Id*. at § 322.007 (a).

[6] *Id.* at § 322.007 (b).

When interpreting these requirements, Texas courts have generally found that an electronic signature is enforceable if the sender signs off on the email with his or her name and if it is reasonably apparent from the context of the communications, or from the parties' actions, which both sides have agreed to conduct transactions electronically. Courts have generally recognized that an email is "signed" if the sender's name is on an email, the email is generated from the sender's email address and closes with at least the sender's first name, or if it contains a header with the sender's name even if the typed name does not appear at the bottom of the email itself. For example, in *Parks v. Seybold*, the Dallas Court of Appeals held that emails concluding with "Thank you, Clyde Parks" immediately above a block containing Parks' full name and contact information sufficiently demonstrated that Parks had signed the emails himself.[7] Although Parks had contended that there was no evidence of any written or "independent" agreement that he had agreed to conduct business transactions electronically, the appellate court disagreed, ruling that the parties' discussions and conduct showed that they agreed to transact business electronically.[8] In *Dittman v. Cerone*, involving an option contract for the sale of property in Harris County, the Corpus Christi Court of Appeals held that a series of three emails constituted an enforceable contract and that the email signature block was a valid "signature".[9] It also found that the record showed that the parties had agreed to conduct business by electronic means.

And now for the fly in the ointment. In a 2011 case, *Cunningham v. Zurich American Insurance*, the Fort Worth Court of Appeals held that the signature line in an email did not constitute a signature.[10] The case involved a breach of contract suit over a purported Rule 11 agreement settling claims in a medical malpractice case on appeal. The case turned on whether an email from one of the insurance carriers' attorneys was actually "signed" and constituted an enforceable agreement under Rule 11. The appellate court observed that "[t]here is nothing to show that the signature block was typed by Grabouski and not generated automatically by her email client."[11] Furthermore, the court noted, "[i]f Grabouski did personally type the signature block at the bottom of the email, nothing in the email suggests that she did so with the intention that the block be her signature." The court declined to hold "that the mere sending by Grabouski of an email containing a signature block satisfies the signature requirement when

[7] 2015 WL 448179 (Tex. App. – Dallas 2015, no writ).

[8] *Id.*

[9] *Dittman v. Cerone*, 2013 WL 865423 (Tex. App. – Corpus Christi 2013).

[10] *Cunningham v. Zurich Am. Ins. Co.*, 352 S.W.3d 519, 529 (Tex. App. – Fort Worth 2011, no writ).

[11] *Id.*

no evidence suggests that the information was typed purposefully rather than generated automatically, that Grabouski intended the typing of her name to be her signature, or that the parties had previously agreed that this action would constitute a signature."[12] Accordingly, the court ruled, the email was not "signed" and so did not meet the requirements of Rule 11.

The *Cunningham* decision has met with sharp criticism. In Williamson *v. Bank* of New York Mellon, the U.S. District Court for the Northern District of Texas dealt with a similar question of whether emails exchanged regarding settlement constituted an agreement enforceable under Rule 11.[13] Applying the UETA and holding that the plaintiff's former attorney's act of signing his email with his typed name was a "signature" within the meaning of the Act, the federal court found that "A typed name at the end of an email is similar to a 'signature' on a telegram, the latter of which can satisfy the statute of frauds."[14] The court specifically rejected the rationale of the *Cunningham* case, reasoning that the attorney created the signature block and directed his email client to attach it to his outgoing emails; that the UETA should be construed broadly; and that permitting a signature block to have the same effect as a typed signature would be consistent with reasonable practices regarding electronic transactions and with the continued application and expansion of these practices.

More recently, in *Khoury v. Tomlinson*, Houston's First Court of Appeals weighed in on the issue of an email signature block as an enforceable signature for purposes of the Statute of Frauds.[15] The *Khoury* case involved an agreement in which John Khoury invested in PetroGulf, a company run by Prentis Tomlinson and which supposedly had a contract to sell oil from Iraq into Syria. After the investment didn't pan out and Tomlinson admitted that the claimed Syria contract did not exist, Khoury and Tomlinson reached a verbal agreement calling for Tomlinson to repay Khoury's investment. Khoury sent an email summarizing the terms of the agreement, and Tomlinson responded "We are in agreement..." However, his name did not appear in the body of the email. Tomlinson failed to repay Khoury resulting in a lawsuit for fraud, breach of contract, and violation of the Texas Securities Act. Although the jury found for Khoury on all three claims, the trial court set aside the breach of contract finding, ruling that

[12] *Id* at 530.

[13] *Williamson v. Bank of New York Mellon*, 947 F. Supp. 704, 710-11 (N.D. Tex. 2013).

[14] *Id.*

[15] *Khoury v. Prentis Tomlinson Jr.*, No. 01-16-00006-cv, (Tex. App. - Houston [1st Dist.] March 30, 2017), http://caselaw.findlaw.com/tx-court-of-appeals/1854824.html.

the Statute of Frauds barred enforcing the oral agreement that was summarized in Khoury's email.

The First Court of Appeals reversed, concluding that the appearance of someone's name or email address in the "From" line of an email constitutes a signature, thus satisfying the Statute of Frauds.[16] The Houston appellate court specifically considered the UETA, case law interpreting the Act, dictionary definitions of the word "sign", as well as the underlying purpose of the Statute of Frauds. Like the *Williamson* case, the *Khoury* holding criticized the *Cunningham* decision, particularly its lack of any explanation for "why physically typing in a signature line at the time of drafting the email should be required for a 'signature block' to constitute a signature."[17] The Houston appellate court concluded that "A signature block in an email performs the same authenticity function as a 'from' field. Accordingly, it satisfies the requirement of a signature under the UETA."[18]

Yet *Cunningham* has never been overruled, resulting in a split of authorities on the issue of email signatures that awaits resolution by either the Supreme Court of Texas or the Legislature. Since a trial court is bound by the decisions of the court of appeals that covers its district, attorneys should carefully consider the venue implications of any dispute that might involve email signatures and the Statute of Frauds. But beyond that, be aware that a typed signature or an email can create an enforceable contract, and counsel your clients (and yourself) accordingly. Out of abundance of caution, you may wish to abandon the "standard" signature block, and create a new one that contains Rule 11 disclaimer language, such as wording that states that your email exchange is not intended to form any agreement between sender and recipient. After all, as the unsettled legal landscape in the area demonstrates, no ink doesn't necessarily mean no problems.

About the Author:

John G. Browning is a shareholder in the Dallas law firm of Passman & Jones, P.C., where he practices a wide variety of civil litigation in state and federal courts. He is the author of three books and numerous articles on social media and the law, and he serves as an adjunct professor at SMU Dedman School of Law and at Texas Tech University School of Law. Mr. Browning's work has been cited by courts across the country and in numerous law review

[16] *Id.*

[17] *Id.*

[18] *Id.*

articles, and publications like The New York Times, TIME magazine, Law 360, and others have quoted him as a leading expert on social media and the law.

A Dozen E-Discovery Strategies for Requesting and Producing Parties

By Craig Ball

Two characteristics that distinguish successful trial lawyers are preparation and strategy.

Strategy is more than simply doing what the rules require and the law allows. Strategy requires we explore our opponent's fears, goals and pain points ... and our own. *Is it just about the money? Can we deflect, distract or, deplete the other side's attention, energy or resources? How can they save face while we get what we want?*

In a world where less than one-in-one-hundred cases are tried, discovery strategy, particularly e-discovery strategy, is more often vital than trial strategy. Yet, strategic use of e-discovery garners little attention, perhaps because the fundamentals demand so much focus, there's little room for flourishes. As lawyers, we tend to cleave to one way of approaching e-discovery and distrust any way not our own. If you only know one way of doing things, how do act strategically?

Strategic discovery is the domain of those who've mastered the tools, techniques and nuances of efficient, effective discovery. That level of engagement, facility and flexibility is rare; but, you can be still be *more* strategic in e-discovery even if you've got a lot to learn.

Here are a dozen e-discovery strategies for requesting and producing parties.

E-Discovery Strategy for Requesting Parties

1. Anticipate sources: Just because you don't know *all* sources of potentially relevant information held by your opponent doesn't mean you can't anticipate *many* such sources.
2. Be specific in your preservation demand. Use it to inform and close doors.
3. Lose the boilerplate discovery request. ESI isn't just another flavor of "document."
4. Set the agenda for meet and confer in writing, and afford sufficient time and direction to respond.
5. Decide if you will discover narrowly, then broaden scope or demand broadly then narrow scope.
6. Be prepared to articulate the objective behind any request, especially for data and metadata.
7. Gear the timing of e-discovery to insure readiness for depositions.

8. Always scrutinize the capabilities and limits of your opponent’s electronic search methodology.
9. Know what you want most: *discovery or sanctions*. You may have to choose.
10. E-discovery is a marathon, not a sprint. Tenacity pays off; but you have to lay the groundwork (i.e., make the proper record) supporting what you seek.
11. Come to court armed with metrics. One good example is better than all your suspicions.
12. Always be prepared to address proportionality objections.

E-Discovery Strategy for Producing Parties

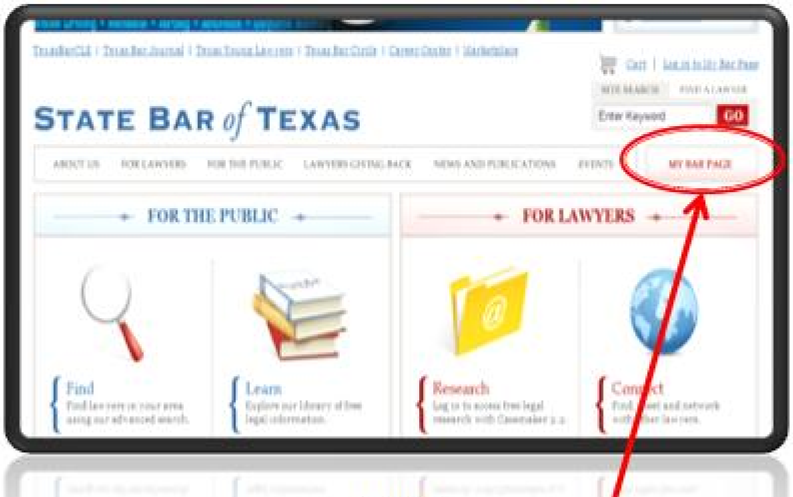
1. Initiate a legal hold immediately, and draft the hold notice with its discovery in mind.
2. Never accept anything is gone without verification, especially when dealing with IT staff.
3. Always respond to preservation demands with a written notice of what you will and won’t do.
4. Be proactive, not merely responsive. Have a reasonable e-discovery plan in place at the outset, and counter unreasonable demands with reasonable proposals.
5. Requesting parties are so anxious to get *something*, they will often agree to *anything* before they appreciate how much it will hurt them. Exploit this, and get their concessions in writing.
6. Seek to shift costs whenever feasible, even when you will not prevail.
7. Come to court armed with metrics. Carefully quantify cost and burden. Use genuine numbers, not absurd extrapolations.
8. Promote use of highly precise keyword searches as they are least helpful to opponents.
9. Test to insure your searches pick up known responsive and privileged items.
10. Avoid categorical representations about ESI as they rarely survive scrutiny.
11. Impose reasonable parameters limiting collection and search (*g.,* custodian, interval, file types).
12. As rational, demand reciprocity in preservation, collection, search and production.

About the Author:

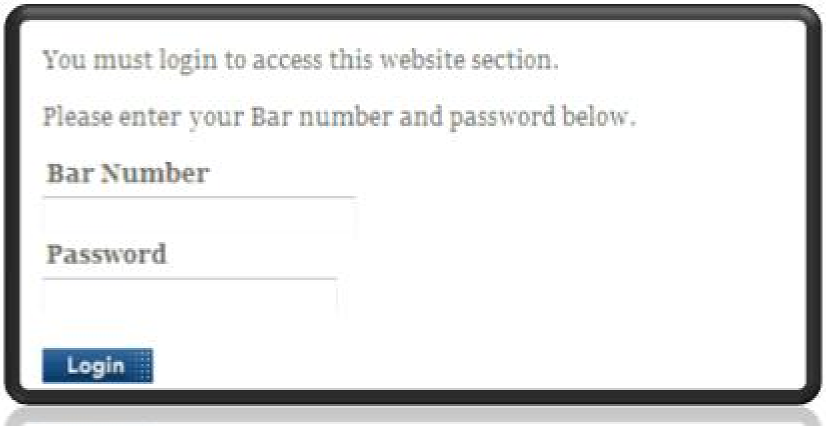
Craig Ball of Austin is a Board-certified trial lawyer who limits his practice to service as a court-appointed Special Master and consultant in computer forensics and electronic discovery. A founder of the Georgetown University Law Center E-Discovery Training Academy, Craig serves on the Academy's faculty 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.

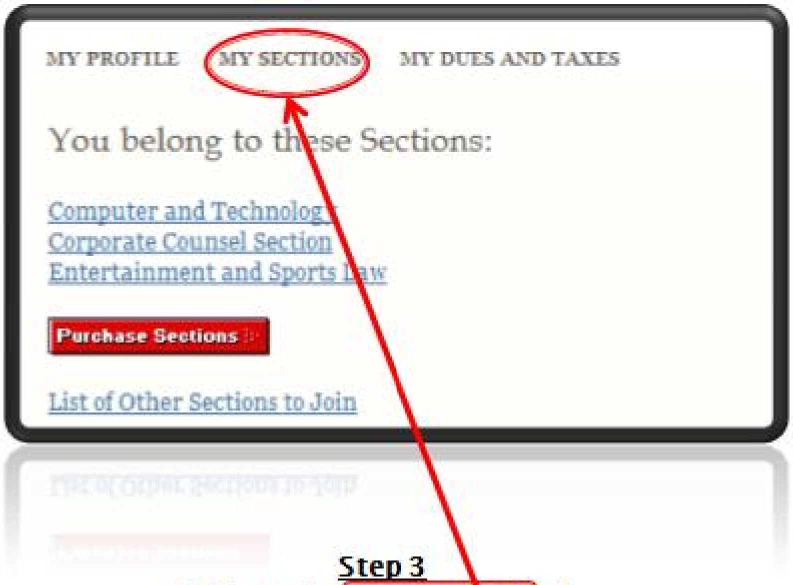
Please enter your Bar number and password below.

Bar Number

Password

Login

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

Shannon Warren – Houston – Chair
Michael Curran – Austin – Chair-Elect
Sammy Ford IV – Houston – Treasurer
John Browning – Dallas – Secretary
Craig Ball – Austin – Past Chair

Term Expiring 2017

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

Term Expiring 2018

Pierre Grosdidier – Houston
David Coker – Dallas
Laura Leonetti – Houston
Reginald Hirsch – Houston

Term Expiring 2019

Sanjeev Kumar– Austin
Judge Xavier Rodriguez– San Antonio
Judge Scott J. Becker– McKinney
Eric Griffin– Dallas

Chairs of the Computer & Technology Section

2016–2017: Shannon Warren
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