COMPUTER AND TECHNOLOGY SECTION

Circuits

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

May 2016

TABLE OF CONTENTS

CLICK ON TITLE TO JUMP TO ARTICLE

Message from the Chair for Circuits May 2016

By Craig Ball, 2015-2016 Chair

This is my last opportunity to preface this fine publication as Chair of the Computer and Technology Section. It's been an honor to serve you, and to work with your brilliant Council. They are not just gifted thought leaders but are exemplary men and women dedicated to serving the Bar and the public. They believe, as I do, that lawyers need not always be late to the party when it comes to emerging technologies. The Bar can embrace technology in law practice to better serve our clients and make legal services more accessible and affordable. Too, we can master the law of technology and confidently and competently guide our clients in areas of privacy, cybersecurity, intellectual property, electronic discovery and a host of other busy, perilous intersections of law and technology.

The legal profession is the frog in the pot of warming water. Oblivious, and unwilling or unable to adapt to social and technological change, lawyers will suffer mightily when the water starts to boil. *Many lawyers, that is; but, not all.* Not *you*. Savvier lawyers embrace change. Technology is your leg up.

I close by recognizing Michael Curran for his commitment to *Circuits* as its Editor. Singlehandedly at first, and later working with Elizabeth Rogers as Co-Editor, Michael has done a splendid job gathering quality articles and assembling them into a useful and engaging newsletter. Thanks to both Michael and Elizabeth for their leadership, and to Antony Ng and Sanjeev Kumar for their editorial support.

COMPUTER AND
TECHNOLOGY
SECTION

Return to Table of Contents

Letter from the Editors

By Elizabeth Rogers and Michael Curran

Along with Cherry Blossoms on the east coast and bluebonnets in Texas, in Chicago, you know that you can count on the annual ABA Tech Show to blossom every spring with a field of the latest innovations in law practice management. A few of our esteemed Council members were able to attend the program during mid-March, marking the Show's 30th anniversary. Stay tuned for several articles they will be submitting over the next few issues of *Circuits* discussing lessons learned over the course of 2½ amazing days jam-packed with programs including security and encryption, social media, e-discovery, law firm management and marketing, finance, workflows, best practices, and cutting-edge technology. We have included Tony Ray's article summarizing the event, in this edition.

A few weeks after the ABA Tech Show, the 2016 International Association of Privacy Professionals Summit was packed with over 3,500 attendees in Washington D.C. There, the program choices included FBI General Counsel James A. Baker's discussion of burning questions about privacy and national security, including the Apple iPhone case, encryption and going dark and a General Session keynote presentation by Brad Smith, Microsoft's Chief Legal Officer, about its battles with the Department of Justice. These types of conferences that focus on issues involving law and technology are occurring across the nation, and we invite those of you who attend these events to submit articles and share your insights.

In the next issue of the *Circuits*, you will also note some new faces on the Council and new Officers providing leadership to our Section membership. We are thrilled to receive so many resumes from incredibly talented lawyers who expressed interest in serving the Section membership. There was pretty stiff competition for the Council openings, but anyone who wants to participate in the Section can join our efforts through work on a committee, by publishing an article, or by participating in events like the State Bar Annual Meeting, which has several sessions sponsored by the Computer & Technology Section. Part of the rewarding task of serving on the Council or being an active Section member is also being able to support the legal community and the community as a whole, throughout Texas, as part of our mission to provide education about the intersection of law and technology. Please submit questions or articles anytime to Michaelcurranpc@gmail.com. Until next time, we hope you enjoy this issue!

Return to Table of Contents

ABA TECHSHOW 2016

By Tony Ray

The American Bar Association's Law Practice Division puts on the ABA TECHSHOW every year. This year was the 30th anniversary of the show. The purpose of ABA TECHSHOW is for lawyers to learn how "technology helps them work smarter, practice better, and deliver higher quality legal services to clients."

ABA TECHSHOW has plenary sessions and educational tracks as well as an exhibitor hall where the latest products and services are shown.

Plenary Sessions

Data breach and cyber security were the main topics for this year's TECHSHOW. The plenary sessions were focused on security with the keynote address given by Cindy Cohn who serves as the Executive Director of the Electronic Frontier Foundation. Another plenary session was titled "Can they hear me now? Practicing law in an age of mass surveillance."

Educational Programs

The educational programs are divided into tracks such as "Starting up/Starting Over," "Cyber Security and Privacy," "Advanced IT" and, "Promoting & Managing Your Practice."

In my own personal opinion, one of the best tracks they had was all about "Fundamentals of Microsoft Office." While the title implies that it would be very basic, it in fact turned out to be a very in-depth study of the Microsoft products that most law offices use. I have been using Microsoft Word for many years and assumed that I knew almost everything about it. After the session on Word, I realized that I knew very little and had a lot to learn. Have you ever wondered what those little small black squares are to the left of a paragraph? They actually symbolize something and now I know what. Why is the formatting on my document always getting messed up? Now I know – it's all because of those pesky little black squares.

Another interesting track concerned Advanced Information Technology where subjects such as "The Deep Dark Web" were covered. I knew what the "Dark Web" was, but I was not familiar with the term "Deep Web." According to the presenters, the Deep Web is where most of the information available on the Internet is located. They analogized it to an iceberg with a typical Google search only searching the very tip of the information. The vast majority of information is below the surface and is not searched by Google. The information is available but you have to know how to access it. Many of these sites, on what the presenters called the Deep Web, are

Return to Table of Contents

government sites where you have to actually go to the site and enter a query to locate the information for which you're looking. Their information is not available for Google to crawl so it doesn't get indexed. Although not indexed by Google, the information is there if you know where to look. They discussed a number of sites that maintain information on where to look for specific information. For instance, there is a site that maintains a list of every city, county, state and federal site that has criminal information on individuals. Many of these index sites are subscription services.

The Dark Web, on the other hand, can be a dangerous and disgusting place that needs to be approached with caution. While there is information that lawyers may need in the Dark Web, it is best to be very cautious when you go there.

The Vendors

You can always tell what the current hot item is in legal technology by the number of vendors who are selling or providing a particular type of product or service. In the past, E-discovery was the big item with companies offering products and services to help with E-discovery. In recent years, cloud storage products and services were big items. This year the big item was practice management. It seemed that every other vendor offered some practice management program or service.

I interviewed Steven J. Best, Affinity Consulting Group LLC for this article. Steven served as the chair of ABA TECHSHOW 2016. Steven is an attorney who switched careers and is now a consultant on, as his website says, "technology audits; strategic business & management assessments; technology selection and implementations; traditional and cloud-based financial practice management; litigation support and trial preparedness; and in-house training and professional development." I wanted to interview Steven about this year's vendors and why they were focused on practice management as the hot topic this year. He indicated that TECHSHOW did not have anything to do with which vendors showed up. The vendors chose to come and show what they thought was important for this year's TECHSHOW. No one was seeking out vendors offering a particular product or service.

Stephen also said that this year's TECHSHOW had tracks catered to small firm lawyers, public lawyers (those who work for legal services and other public organizations) and in-house lawyers. These tracks were in addition to tracks of interest to big law firms such as Cybersecurity, Advanced IT, etc.

He said a month after the show he was still getting emails from people telling him how much they enjoyed the show and how much they learned from it. I can second that. I would recommend TECHSHOW to all attorneys who are interested in keeping abreast of technology tools in the law department and legal developments involving technology. TECHSHOW is held every year in Chicago in the spring. Their website is http://www.techshow.com/.

About the Author:

Robert A. Ray of Tyler limits his practice to litigation involving inheritance disputes, related property disputes and associated torts. He is Board Certified – Personal Injury Trial Law. He is past Chair of the State Bar Computer & Technology Section. He is a winner of a Lifetime Achievement in Technology Award from the Section. He was appointed by the Chief Justice of the Texas Supreme Court to serve as an ex officio member of the Judicial Committee on Information Technology. For more information, please visit his website www.TexasInheritance.Com or his blog www.InheritanceLaws.Info.

Attention FinTech: Why “Compliance by Design” Must Be On Your Roadmap

By Erin Fonte, Elizabeth Khalil and Jacqueline Allen

Non-financial companies continue to enter the mobile/emerging/alternative payments and financial technology (“FinTech”) space in increasing numbers. Many entrants – particularly those from a tech background in unregulated or lightly regulated industries – are surprised to learn that all or part of their products and services are regulated. We have seen this occur with several of our FinTech clients over the last few years, and typically these FinTech companies go through what we have labeled “The 5 Stages of FinTech Startup Grief”:

- **Denial** (“No, we are just pushing a button on the app and using technology to move money, and funds are only in our bank account for a split second – how can that be regulated?”)
- **Anger** (“What do you mean the seamless payment function central to my killer app is regulated, and there may be potential criminal penalties for unlicensed money transmission?”)
- **Bargaining** (“Wait, maybe we can design or hack around the regulation or licensing requirement.” [NOTE: And see how well that ultimately worked for the founder and former CEO of Zenefits as discussed in more detail below.])
- **Depression** (“I can’t believe we have to spend money on legal and delay our launch date [*pulls hoodie around face*].”)
- Finally, **Acceptance** (“Okay, I guess the licensing requirements and potential criminal penalties are real and we need to get compliant.”)

Many FinTech companies believe they offer completely new products and services, but a new channel is not necessarily a new product or service. When you get behind the user interface and API, and really get under the hood, one or more of the underlying *activities* being carried out is often not new, and is already subject to one or more existing laws, regulations, and/or regulatory guidance/best practices.

Several agencies at both the federal and state level have supervision and enforcement authority over these laws and regulations. The authority of these agencies can extend *directly* to FinTech companies and is not limited to only financial institutions – the Consumer Financial Protection Bureau in particular has broad enforcement authority for any company that offers a consumer-facing financial product or service. Direct regulation is often triggered by certain underlying activities (e.g., money transmission).

FinTech companies are often also *indirectly* regulated because they are either a customer of, or are partnering with, regulated financial institutions. As a bank or credit union customer (what companies must do to access debit/credit card rails, automated clearing house transactions, and wires to carry out certain core functions of their products or services), the bank/credit union has to undertake a due diligence analysis of the FinTech company's line of business and associated risks. If a bank or credit union is deemed to be a "third party payment processor" or "third party service provider" (i.e., carrying out certain activities on behalf of the FinTech's customers, who are not customers of the bank), additional due diligence and oversight is required by banking/credit union regulations and often also by payment network rules.

If the FinTech company is going to partner with a bank/credit union (e.g., as a distributor of a physical or virtual prepaid account issued by the bank, as itself an issuer of a mobile "access device" to originate transactions to depository or credit accounts or to provision a bank/credit union's debit, credit or stored value cards into the FinTech company's mobile wallet), then the FinTech company is a "third party vendor" to the financial institution. There are many laws, rules and regulations and compliance obligations that the bank/credit union is required *by law* to "pass through" to the FinTech company, such as information security and privacy requirements under the federal Gramm-Leach-Bliley Act.

FinTech companies should, at a minimum, determine whether all or a portion of their products or services may trigger any of the following laws and regulations (and remember, you have to read the laws and regulations AND understand the applicable agency's interpretation of those laws and regulations):

- <u>Bank Secrecy Act (BSA)/anti-money laundering (AML) requirements and OFAC requirements</u>: The FinTech company may have to obtain information about the financial institution's customer identification program as required under the Bank Secrecy Act.
- <u>Privacy and data security laws and regulations, including, but limited to, the Gramm-Leach-Bliley Act</u>: If a FinTech company collects or shares personal and/or financial information, the company may be required to comply with various federal and state privacy and data security laws and regulations – and watch out for implications of geolocation data.
- <u>Federal money service business and state money transmitter laws and regulations</u>: If the FinTech company touches money intended for others, such as transmitting money or selling or issuing payment instruments (e.g., prepaid cards), the FinTech company may

need to register with FinCEN as a federal money service business, or become licensed under and comply with state money transmission laws.

- Federal and state lending laws: If the FinTech company extends credit or provides services to someone who extends credit, the company may be subject to federal and state lending and/or brokering laws. The company may also be required to obtain a state license to extend credit or broker loans.
- Electronic Funds Transfer Act/Regulation E: If the FinTech company offers services that allow consumers to transfer money to or from certain accounts, or purchase prepaid cards (including, but not limited to, gift cards), or transfer money internationally, the company will be required to comply with federal consumer protection laws under the Electronic Fund Transfer Act and Regulation E.
- State prepaid and gift card laws: If the FinTech company sells prepaid or virtualized card accounts, including, but not limited to, gift cards, there are various state laws imposing disclosure requirements, fee limitations, and unclaimed property reporting obligations that may apply to the company.
- Federal prohibition against Unfair, Deceptive [or Abusive] Acts or Practices (UDAAP): Regardless of the type of product offered, FinTech companies must also be aware of the Federal Trade Commission's prohibition against Unfair or Deceptive Acts or Practices, as well as the Consumer Financial Protection Bureau's Unfair, Deceptive or Abusive Acts or Practices. These laws can always be enforced directly against FinTech companies (see CFPB enforcement action against Dwolla below).
- Other industry or specific product laws, rules and regulation: If a FinTech company engages in other types of services that are regulated to a greater or lesser extent, such as insurance, employment benefits, investment or retirement account operations or services, or securities (including specific types of crowdfunding), odds are the applicable regulatory regimes for those industries and products will apply as well.

We highlight these issues not to be negative or to dishearten to FinTech startups, but rather to help arm them with the right tools so they can design products and services to be "compliant by design." While there is a lot of debate about whether regulation and enforcement is stifling innovation, or whether tech companies have an unfair advantage due to less oversight by regulators, what is certain is that regulators at the state and federal levels are paying attention. Two recent headlines provide good reminders of why it is important to be "compliant by design."

Return to Table of Contents

Dwolla Enforcement Action

The Consumer Financial Protection Bureau ("CFPB") made headlines in March 2016 by taking action against Dwolla, an online and mobile payments platform. The CFPB imposed a $100,000 penalty against Dwolla, and while the dollar amount of the penalty is small compared to other civil money penalties imposed on banks, the action is significant because the CFPB has essentially staked out its turf in regulating data security for non-financial institutions. It is direct reminder of the CFPB's broad enforcement powers under the Dodd-Frank Act. While the CFPB lacks authority over the substantive data security requirements that are enforced by the federal financial regulators, that is no obstacle to the CFPB's ability to take an action like this, which was initiated under its authority to police "deceptive" acts or practices.

Dwolla's services allow users to direct Dwolla to transfer funds to another consumer or merchant from either funds in the user's Dwolla account, or from the user's personal bank account linked to the user's Dwolla account. Users can send transfers either online or through the Dwolla mobile app, and ultimate settlement of transactions is typically done via the ACH network.

Users must provide various pieces of personal information to use Dwolla, such as name, address, date of birth, telephone number, and Social Security Number. To link a demand deposit account to a Dwolla account, users must also provide their bank account number and routing number.

Despite making numerous representations regarding the safety and security of users' personal information, the CFPB found that such representations were not true. According to the CFPB, Dwolla deceived consumers and misrepresented its data security practices simply by making these misleading statements alone, without the necessity of committing an actual data security breach or compromise. For example, the CFPB's consent order states Dwolla made the following representations either on its website or in direct communications with consumers:

- Dwolla's data security practices "exceed industry standards" or "surpass industry security standards";
- Dwolla "sets a new precedent for the industry for safety and security";
- Dwolla stores consumer information "in a bank-level hosting and security environment";
- Dwolla encrypts data "utilizing the same standards required by the federal government" and "all sensitive information that exists on its servers";
- "All information is securely encrypted and stored";

- Dwolla is "PCI Compliant"; and
- Dwolla "encrypt[s] data in transit and at rest."

In fact, Dwolla did *not* encrypt all sensitive personal information at rest, and Dwolla was not PCI compliant. Specifically, Dwolla failed to encrypt the following data fields, either in transit or rest:

- First and last name;
- Mailing addresses;
- 4-digit PINs used to access Dwolla accounts;
- Social Security numbers;
- Bank account information; and
- Digital images of driver's licenses, Social Security cards, and utility bills.

Dwolla also encouraged its users to submit sensitive personal information through email, in clear text, such as Social Security numbers and scanned images of driver's licenses, utility bills, and passports. For several years, Dwolla failed to adopt or implement data-security policies and procedures, or a written data-security plan. Dwolla also failed to conduct regular risk assessments to identify internal and external risks to consumers' personal information and assess the safeguards in place to control such risks.

The CFPB found that Dwolla's representations regarding its data security practices constituted deceptive acts or practices in violation of the Consumer Financial Protection Act. The Federal Trade Commission, which has enforcement authority over non-bank financial institutions under the Gramm-Leach-Bliley Act, has previously obtained several data security settlement agreements resulting from violations of the prohibition against unfair or deceptive acts or practices under the Federal Trade Commission Act, but this is a enforcement action "of first impression" for the CFPB.

The CFPB is requiring Dwolla to take the following actions, among others:

1) Stop misrepresenting its data security practices;
2) Adopt and implement reasonable and appropriate data-security measures to protect consumers' personal information;
3) Establish, implement, and maintain a written, comprehensive data-security plan and appropriate data security policies and procedures;
4) Designate a qualified person to coordinate and be accountable for the data-security program;

5) Evaluate and adjust the data-security program in light of the results of risk assessments and monitoring;
6) Conduct regular, mandatory employee training on data-security policies and procedures, safe handling of consumers' sensitive personal information, and secure software design, development and testing;
7) Develop, implement, and maintain an appropriate method of customer identity authentication at the registration phase and before effecting a funds transfer;
8) Develop, implement, and maintain reasonable procedures for selecting and retaining service providers capable of maintaining adequate security practices; and
9) Obtain an annual data-security audit from an independent, qualified third-party.

Dwolla was also required to pay a $100,000 civil money penalty and meet various reporting, recordkeeping, and compliance monitoring requirements for several years.

Zenefits Investigation

The California Department of Insurance recently began an investigation into Zenefits' compliance with health insurance licensure requirements. Zenefits, which is an intermediary in the employee benefits and health insurance industry, employed individuals aspiring to obtain health insurance broker licenses in California and Washington. Zenefits recently self-reported to the California Department of Insurance that some employees used a software tool to complete the online training required for licensure in less than the 52 hours that were legally required to obtain the license. Parker Conrad, the Zenefits' co-founder and former CEO, allegedly helped create a tool for employees to fake the online training completion by faking out the online training system. When this "compliance hack" was discovered, Parker Conrad was pressured by key investors to resign.

Speaking about the Zenefits investigation, California Insurance Commissioner Dave Jones warned that "[n]ew technologies and new business models can bring value and convenience to California consumers, but businesses deploying new technologies and new business models must comply with California's strong consumer protection laws." The State of Washington has also indicated that it is actively investigating Zenefits regarding compliance issues with Washington's laws and regulatory requirements.

The cautionary tale here is that trying to be too clever by half with regard to compliance obligations can often backfire and cause more problems, bad press and economic fallout than the time, cost and effort of just meeting compliance obligations in the first place.

Consumer Complaints

Besides the risk of an enforcement action or government investigation, FinTech companies also risk having consumer complaints filed against them with various regulators. The Federal Trade Commission has long permitted consumers to report unfair business practices. The CFPB recently began accepting complaints against online marketplace lenders and was already accepting complaints pertaining to prepaid cards, money transfers, virtual currency, and other financial services. Anytime a consumer files a complaint with a regulator, it creates a red flag with the regulator that the entity against which the complaint is filed may need to be monitored more closely.

Conclusion

We are in an incredibly exciting and innovative time that is fundamentally re-shaping the way financial products and services are delivered to consumers and businesses. But in carrying the innovation banner forward, FinTech companies must also determine if their products and services are subject to federal and state laws and regulations, which are often rooted in reducing risk to the financial system and risk of harm to consumers and businesses.

When such laws and regulations apply, FinTech counsel often ask regulators to think about alternative ways companies can make disclosures and obtain informed consent, such as incorporating "just-in-time" permissions or decisioning within the app. And that means regulators need to understand consumer use of and interaction with new technologies. Changing technologies require all stakeholders to evolve on many regulatory and compliance issues, particularly on issues of security, authentication, authorization, disclosures and informed consent.

FinTech companies should incorporate appropriate policies, procedures, and controls for their products and services to be "compliant by design." Companies should review all advertising and marketing materials, as well as content displayed on the company's website and in the company's mobile app – and don't try to be too clever or cutesy. Statements like "Security – don't worry, you're good" may do more harm than good by introducing lack of clarity. For example, does "you're good" mean the FinTech company employs best-in-class security, or merely industry standard security?

The risks of failing to comply with applicable laws, regulations, and guidance may include enforcement actions, regulatory investigations, and consumer complaints – all of which can be costly and time consuming to address. Why get ambushed by something post-launch that could have been easily addressed in the process flow from Day 1?

About the Author:

Erin Fonte is the head of Dykema Cox Smith’s Financial Services Regulatory and Compliance Group and a member in the firm’s Austin office, where she assists clients with a broad range of matters related to payments/payment systems, digital commerce, banking and financial services, technology/Internet products, privacy and data protection laws, and general corporate matters.

Elizabeth Khalil is a member in the Chicago office of Dykema Cox Smith, where she is a member of Dykema Cox Smith’s Government Policy Group and Regulated Industries Department. She focuses her practice on all aspects of financial institution regulation, with a particular emphasis on compliance matters.

Jacqueline Allen is an associate in the Dallas office of Dykema Cox Smith, where she advises FinTech companies, money transmitters, non-depository lenders, mobile wallet providers, payment processors, and other technology companies in compliance and regulatory matters, with a particular focus on e-commerce, consumer protection, and privacy and data security.

Return to Table of Contents

State Bad Faith Patent Assertion Laws

By Antony P. Ng

Patent law is generally under federal jurisdiction; but, state lawmakers have become concerned about what they perceive as abusive practices by patent assertion entities (a.k.a. patent trolls) that send out hundreds if not thousands of demand letters alleging patent infringement and threatening a lawsuit unless paid.

For example, Innovatio IP Ventures, LLC sent over 13,000 letters to end-users, including small businesses and restaurants, demanding payment for providing Wi-Fi. These demand letters threatened that, unless the recipient pays licensing fees within two weeks, the recipient will be sued and will have to engage in costly litigation.

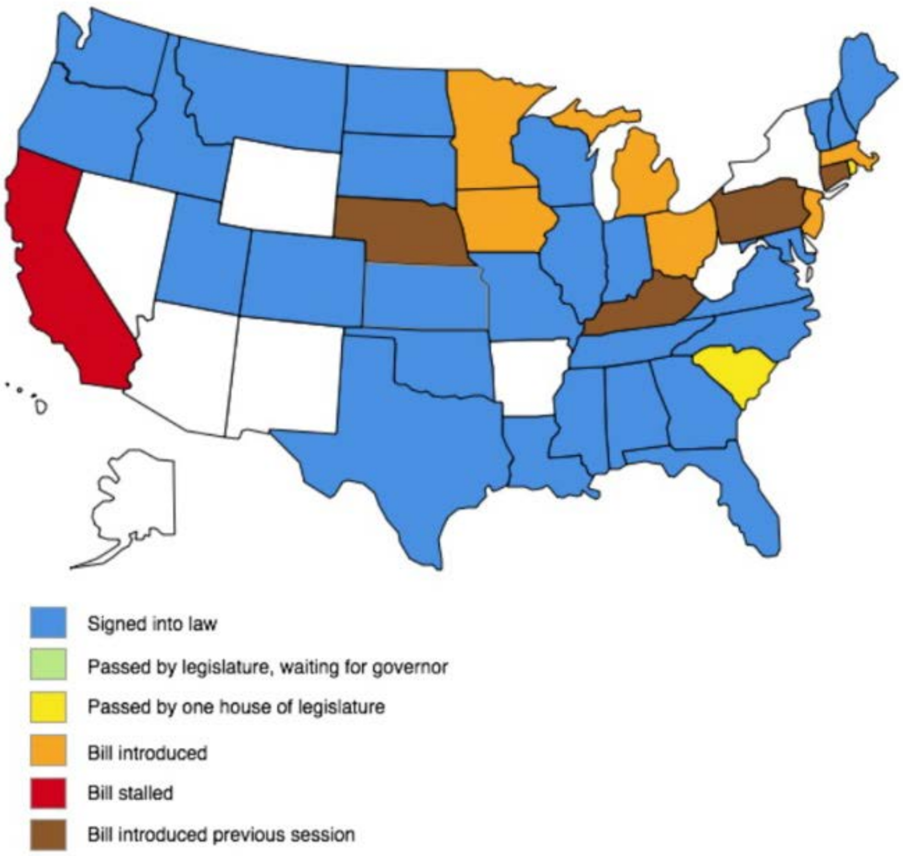
As another example, MPHJ Technology Investments, LLC sent over 16,000 letters to small businesses nationwide demanding payment for using the basic technology of scanning documents to email. In their demand letters, MPHJ misleadingly informed the recipients that "most businesses, upon being informed that they are infringing ... are interested in operating lawfully and taking a license promptly."

Because most consumers and many small businesses lack the expertise to recognize these demand letters as empty threats, they pay the licensing fees to avoid incurring the high cost of patent litigation.

In May 2013, Vermont became the first state to pass legislation for punishing bad faith patent assertions, hoping to reduce the practice of patent trolling. Armed with this new law, the State of Vermont had taken on patent assertion entities such as MPHJ Technology Investments, LLC. MPHJ wrote to about seventy-five businesses in Vermont, alleging infringement by anyone using an office copy machine that automatically scans documents and sends them as emailed attachments. Vermont's Attorney General filed suit against MPHJ in state court for unfair and deceptive trade practices under the Vermont Consumer Protection Act. MPHJ removed case to district court, asserting federal question and diversity jurisdiction. The District court granted Vermont's motion to remand the case back to state court (*see Vermont v. MPHJ Technology Investments, LLC,* 763 F.3d 1350 (Fed. Cir. 2014)).

After Vermont, twenty-seven states, including Texas, have also introduced legislation to create or to amend state law to punish bad faith patent assertions.

Return to Table of Contents


Signed into law
Passed by legislature, waiting for governor
Passed by one house of legislature
Bill introduced
Bill stalled
Bill introduced previous session

Source: Patent Progress, CCIA

These state laws vary in scope but are intended to target the practice of sending vague and deceptive demand letters to coerce inexperienced parties into paying licensing fees. Some states allow only the state attorney general to bring suits for bad faith patent assertions. Other states create private causes of actions, allowing the recipients of demand letters to seek equitable relief, costs and fees, and damages. Some states provide specific examples of what constitutes bad faith claims. Other states list various factors a court may take into account in determining whether a claim is made in bad faith. There are also states requiring a person to post bond if the opposing party shows a reasonable likelihood that it is a bad faith assertion of patent infringement.

Effective September 1, 2015, Texas prohibits sending demand letters that allege a claim of patent infringement in bad faith (*see* §§ 17.951 – 17.955 of Texas Business and Commerce Code). The Texas statute defines bad faith claims of patent infringement to include communications that:

- falsely state that the sender has filed a lawsuit in connection with the claim;
- make a claim that is objectively baseless; and

Return to Table of Contents

- are likely to materially mislead a recipient because of the communications.

The Texas statute further states a claim is objectively baseless when the sender, or the person represented by the sender, lacks current patent licensing or enforcement rights, the patent at issue has been held invalid or unenforceable, or when all of the allegedly infringing activity occurred after the patent at issue expired. In addition, a demand letter is materially misleading when it lacks material information regarding who is asserting the claim, the patent allegedly infringed and the product, service or technology that is allegedly infringing the patent.

The Texas statute allows the Texas Attorney General—and only the Attorney General—to bring an action on behalf of the state seeking civil penalty for bad faith patent assertions. In other words, the Texas statute does not provide a private cause of action.

Penalties include injunctions and up to US $50,000 for each violation, as well as reimbursement for the cost of investigation and prosecution. While the Texas statute does not provide any private cause of action, the Attorney General can seek restitution for a victim's legal and professional expenses related to the bad faith infringement claim.

About the Author:

Antony P. Ng is a registered patent attorney residing in Austin, Texas. He is also an Adjunct Professor at South Texas College of Law where he teaches Internet Law.

Return to Table of Contents

Deduplication: Why Computers See Differences in Files that Look Alike

By Craig Ball

Most people regard a Word document file, a PDF or TIFF image made from the document file, a printout of the file and a scan of the printout as being essentially “the same thing.” Understandably, they focus on content and pay little heed to form. But when it comes to electronically stored information, the form of the data—the structure, encoding and medium employed to store and deliver content—matters a great deal. As data, a Word document and its imaged counterpart are radically different from one another and from a digital scan of a paper printout. *Visually*, they are alike as an image or printout; but *digitally*, they bear not the slightest resemblance.

Hashing

Because Electronically Stored Information or ESI is just a bunch of numbers, we can use algorithms (mathematical formulas) to distill and compare those numbers. In e-discovery, one of the most used and -useful family of algorithm are those which manipulate the very long numbers that comprise the content of files (the “message”) in order to generate a smaller, fixed length value called a “Message Digest” or “hash value.” The calculation process is called “hashing,” and the most common hash algorithms in use in e-discovery are **MD5** (for Message Digest five) and **SHA-1** (for Secure Hash Algorithm one).

Using hash algorithms, any volume of data from the tiniest file to the contents of entire hard drives and beyond can be uniquely expressed as an alphanumeric sequence of fixed length. When I say “fixed length,” I mean that no matter how large or small the volume of data in the file, the hash value computed will (in the case of MD5) be distilled to a value written as 32 hexadecimal characters (0-9 and A-F). It’s hard to understand until you’ve figured out Base16; but, those 32 characters represent 340 *trillion, trillion, trillion* different possible values (2^{128} or 16^{32}).

Hash algorithms are one-way calculations, meaning that although the hash value identifies just one sequence of data, it reveals nothing about the data; much as a fingerprint uniquely identifies an individual but reveals nothing about their appearance or personality.

Hash algorithms are simple in their operation: a number is inputted (and here, the “number” might be the contents of a file, a group of files, i.e., all files produced to the other side, or the contents of an entire hard drive or server storage array), and a value of fixed length emerges at a speed commensurate with the volume of data being hashed.

For example, the MD5 hash value of Lincoln's Gettysburg Address in plain (Notepad) text is E7753A4E97B962B36F0B2A7C0D0DB8E8. Anyone, anywhere performing the same calculation on the same data will get the same unique value in a fraction of a second. But change "Four score and seven" to "Five score" and the hash becomes 8A5EF7E9186DCD9CF618343ECF7BD00A. However subtle the alteration—an omitted period or extra space—the hash value changes markedly. Hashing sounds like rocket science—and it's a miraculous achievement—but it's very much a routine operation, and the programs used to generate digital fingerprints are freely available and easy to use. Hashing lies invisibly at the heart of everyone's computer and Internet activities and supports processes vitally important to electronic discovery, including identification, filtering, Bates numbering, authentication and deduplication.

Hashing for Deduplication

A modern hard drive holds trillions of bytes, and even a single Outlook e-mail container file typically comprises billions of bytes. Accordingly, it's easier and faster to compare 32-character/16 byte "fingerprints" of voluminous data than to compare the data itself, particularly as the comparisons must be made repeatedly when information is collected and processed in e-discovery. In practice, each file ingested and item extracted is hashed and its hash value compared to the hash values of items previously ingested and extracted to determine if the file or item has been seen before. The first file, sometimes called the "pivot file," is hashed and subsequent files with matching hashes are suppressed as duplicates. Each duplicate and its metadata is then logged and added to a database.

When the data is loose files and attachments, a hash algorithm tends to be applied to the full content of the files. Notice that I said to "*content*." Some data we associate with files is not actually stored inside the file but must be gathered from the file system of the device storing the data. Such "system metadata" is not contained within the file and, thus, is not included in the calculation when the file's content is hashed. A file's name is perhaps the best example of this. Recall that even slight differences in files cause them to generate different hash values. But, since a file's name is not typically housed within the file, you can change a file's name without altering its hash value.

So, the ability of hash algorithms to deduplicate depends upon whether the numeric values that serve as building blocks for the data differ from file-to-file. Keep that firmly in mind as we consider the many forms in which the informational payload of a document may manifest.

A Word .DOCX document is constructed of a mix of text and rich media encoded in Extensible Markup Language (XML), then compressed using the ubiquitous Zip compression algorithm. It's a file designed to be read by Microsoft Word.

When you print the "same" Word document to an Adobe PDF format, the Word document is reconstructed in a *page description language* specifically designed to work with Adobe Acrobat. The PDF file is encoded and compressed in an entirely different way than the original Word file.

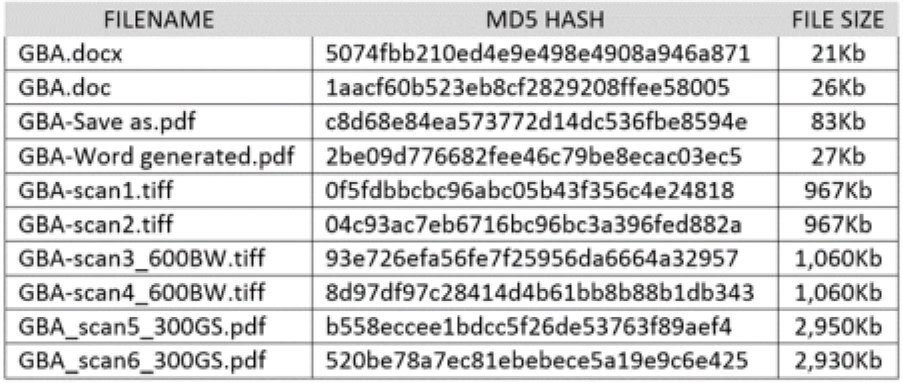
When you take the printed version of the Word document and scan it to a Tagged Image File Format (TIFF), you've taken a picture of the document. It's now constructed in yet another different format—one designed for TIFF viewer applications.

To the uninitiated, they are all the "same" document and might look pretty much the same printed to paper; but as with ESI, their structures and encoding schemes are much different. Moreover, even files generated in the same format may not be *digitally* identical when made at different times. For example, no two optical scans of a document will produce matching hash values because there will always be some variation in the data acquired from scan to scan. Small differences perhaps; but, any difference at all in content is going to frustrate the ability to generate matching hash values.

To illustrate this, I created a Word document of the text of Lincoln's Gettysburg Address. First, I saved it in the latest .DOCX Word format. Then, I saved a copy in the older .DOC Word format. Next, I saved the Word document to a .PDF format, using both the Save as PDF and Print to PDF methods. Finally, I printed and scanned the document to TIFF and PDF. Without shifting the document on the scanner, I scanned it several times at matching and differing resolutions.

I then hashed all the iterations of the "same" document and, as the table below reveals, none had matching hash values, not even the successive scans of the unshifted paper document:

Return to Table of Contents



FILENAME	MD5 HASH	FILE SIZE
GBA.docx	5074fbb210ed4e9e498e4908a946a871	21Kb
GBA.doc	1aacf60b523eb8cf2829208ffee58005	26Kb
GBA-Save as.pdf	c8d68e84ea573772d14dc536fbe8594e	83Kb
GBA-Word generated.pdf	2be09d776682fee46c79be8ecac03ec5	27Kb
GBA-scan1.tiff	0f5fdbbcbc96abc05b43f356c4e24818	967Kb
GBA-scan2.tiff	04c93ac7eb6716bc96bc3a396fed882a	967Kb
GBA-scan3_600BW.tiff	93e726efa56fe7f25956da6664a32957	1,060Kb
GBA-scan4_600BW.tiff	8d97df97c28414d4b61bb8b88b1db343	1,060Kb
GBA_scan5_300GS.pdf	b558eccee1bdcc5f26de53763f89aef4	2,950Kb
GBA_scan6_300GS.pdf	520be78a7ec81ebebece5a19e9c6e425	2,930Kb

Thus, file hash matching—the simplest and most defensible approach to deduplication—will not serve to deduplicate the “same” document when it takes different forms or is made optically at different times.

Now, here’s where it can get confusing. If you copied any of the electronic *files* listed above, the duplicate files would hash match the source originals, and would handily deduplicate by hash. Consequently, multiple copies of the same electronic files will deduplicate, but that is because the files being compared have the same *digital* content. So, we must be careful to distinguish the identicality seen in multiple iterations of the same file from the pronounced differences seen when different electronic versions are generated at different times from the same content.

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.

Return to Table of Contents

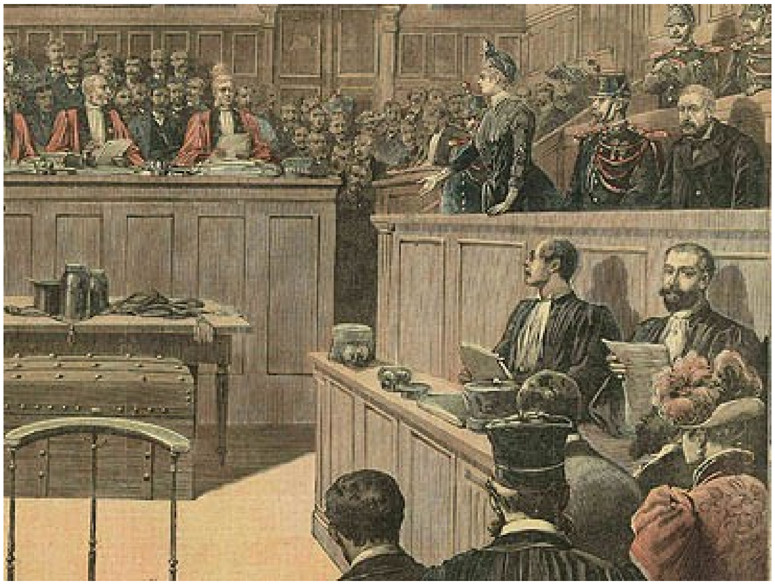
Emerging Standards of Technical Competence

By Ronald L. Chichester

Introduction

Lawyers were "knowledge workers" before that cliché was first coined.[1] Knowledge workers generally require three types of thinking: convergent (correctly answer factual questions); divergent (generate possible solutions from a given situation); and creative (come up with novel solutions to problems). Quite often, all three types of thinking are evident in a lawyer's work product. Indeed, it was this ability to use the three types of thinking that set lawyers (and other knowledge workers) apart.

A century ago, only the client or a court consumed the work product generated by lawyers. The information in a legal brief started in the lawyer's head, was spoken to his secretary, transcribed to paper, presented to the client or court, filed away in a cabinet, moved to a box, and then finally moved to a landfill. Much of the knowledge distilled by the attorney went to waste. Clients often sought out lawyers who had tried similar cases in an attempt to leverage past work. Such was the state of the art in those days.



The Gouffé Case, circa 1890, available at http://traitsdejustice.bpi.fr/home.php?id=4

[1] The phrase was first coined by Peter Drucker. *See*, Peter F. Drucker, THE LANDMARKS OF TOMORROW (New York: Harper and Row 1959).

More Recent History

The advent of computers began to change the practice of law in the 1980's, after computers had largely automated some of the other professions, particularly engineering.[2] At first, attorneys viewed computers as being beneath them. They were glorified devices fit only for their secretaries. Even as late as the mid 1990's, some law firms required – as their standard practice – the deletion of a document once it had been printed. In short, the personal computer (PC) was just a very expensive typewriter. There was one area, however, where computers made perfect sense – legal research. Cases and scholarly articles were cataloged electronically and, by 1990, law schools were teaching students how to perform *keyword searches using Boolean logic*.

As PC's became more pervasive, many attorneys were assigned one whether they wanted it or not, in some cases relegating many PC's to use as expensive paperweights. Eventually, (grudgingly) attorneys began using personal computers to draft their own documents, with a corresponding increase in the attorney-to-secretary ratio. An attorney's skill with a word processor soon became *de rigueur*. On the one hand, the concept of cut/copy/paste enabled chunks of older work product to be re-used in other cases, saving time. On the other hand, personal computers turned out to be wonderful tools for procrastination, wherein the time that could have been saved was converted into time for more revisions, so briefs took just as long to write although ostensibly of higher quality.

By the mid-1990's, the electronic files that were generated by attorneys were moved off onto central storage devices. This led to yet another concept – cut/copy/paste of one's work product by other attorneys. However, the internal structure of most major law firms discouraged an attorney from sharing his work product with partners and associates who, for all intents and purposes, competed with each other. The structure of law firms did not enable the original attorney to get a "cut" of time when an associate utilized the information in their electronic file. This was yet another instance where the old style practice of keeping knowledge

[2] The author was an aerospace engineer in the 1980's, and witnessed the automation of the engineering profession first hand. He recalls the stories that his bosses regaled him when they were junior engineers. They had all started out as human calculators (using slide rules) to perform calculations for more senior engineers. Hand-held calculators ended that practice – and hundreds of jobs with it. By the time that the author was in his twenties, it was possible for a small team of talented engineers to design (from scratch) an F-16 class airplane in two weeks – a task that theretofore had taken hundreds of engineers years to accomplish.

scarce (to enhance its value) clashed with technology (which made the sharing of information nearly free).

Long term storage of electronic files also led to the concept of search engines and indexing (so that the other attorney could find the right file in the first place). The 90's also brought us the biggest time-killer of them all: email. Clients loved email, and soon attorneys could not get away from it. Blackberrys went from being a gadget to indispensable. Then along came attachments for email, and this gave new life to under-utilized disk space and created a market for de-duplication in the burgeoning field of e-discovery. Yet it was email that prompted attorneys to become adept at *communication* and data *format*. The right version of the electronic file needed to get to the right client (and <u>not</u> opposing counsel), and had to be readable by the client's suite of software. Incidentally, clients now realize that the attorney's work product can be added to their own storehouse of knowledge, and lawyers should know that their knowledge will be *data mined* both by clients and other attorneys.

Attorneys were not the only ones using computers. Indeed, well over 90% of litigation documents were first generated in electronic form. Consequently, the field of e-discovery has generated a bevy of technologies requiring the litigator's attention. There arose terms such as *metadata, native format, structured and unstructured data, databases, content management systems* and *keyword searches* that could engender malpractice difficulties if not handled correctly. Later came *predictive coding* and *automated document review*, the boon of partners and the bane of young associates.

Today, the Internet acts as the penultimate central server, where an attorney's newly acquired communication and formatting skills could be leveraged for yet another concept: *collaboration*. Yes, cooperation in the inherently adversarial. Attorneys and opposing counsel are now encouraged to "work together" on a document that settles a dispute or transaction between their respective clients, which led to another malpractice "gotcha" – *document metadata*. Because metadata is data about data, and past edits that are stored by word processors is metadata that can be discovered by the opposing counsel, such metadata can be a nasty surprise (with ethical implications) for the unwary. Competent transaction attorneys had to become adept at metadata laundering, but real-time collaboration complicates the ethical issues for transactional attorneys significantly.

The late 1990's and early 2000's brought us the horrors of widespread hacking on the Internet, and so attorneys now have to learn about *encryption*. Encryption became the tool of choice after California enacted the first data breach/notification law in 2003, with all but three states having followed suit within a decade. Unfortunately, law firms were found to be great victims for hackers, because the firm's servers proved to be a "target rich" environment that was relatively unprotected. The infamous breach of Target's headquarters highlighted the vulnerabilities that clients faced with their supplier's lack of security measures. The Target breach and others have prompted insurance carriers to conduct *security audits* of law firms. Managing partners now have to grapple with details about *firewalls*, *IT controls*, and *incidence response* policies. Statutory data breach/notification laws are also forcing attorneys to appreciate the *privacy* implications of their data retention policies, and how they store and protect their client confidences as well as sensitive financial and health data.

The Future

Thirty years ago, I witnessed – first hand – how the profession of engineering was automated. I was a young engineer, fresh out of the University of Michigan, delighted to know that I was a member of a small team of engineers at General Dynamics who could design (from scratch) an F-16-class airplane in two weeks. While we marveled at our abilities, we lost sight of the fact that we had cleverly worked ourselves out of a job. I got out of that profession while I could and went to law school, thinking that the legal profession was immune to similar misfortune. Alas, I was wrong.

There is a phrase, often attributed to Joseph Stalin, that "quantity has a quality all its own." In a recent book by Martin Ford[3], he cites Moore's Law, "the well-established rule of thumb that says computing power roughly doubles every eighteen to twenty-four months" and suggests that "not everyone has assimilated the implications of this extraordinary exponential process."[4] He employed the simile of a traveling car. For the first minute, you drive at 5 mph and cover 440 feet. Ford notes that Moore's Law has been in effect since 1958 (the year of the first integrated circuit), so by comparison, cars today would be traveling at 671 *million* miles per hour and cover more than 11 million miles per minute. Ford rightly points out that there is an entirely different character – and capability – between the first minute and the twenty-eighth minute, and that there is a similar different character and capability in computing between 1958 and today. Quantity, indeed, has a quality all its own.

[3] Martin Ford, RISE OF THE ROBOTS" (Basic Books, 2015).

[4] Ford, at xii.

Both Ford and Jaron Lanier[5] point out that the Internet has resulted in a net *loss* of jobs. Ford goes further, and cites statistics that in the first decade of the twenty-first century, *no* net jobs were added in the United States, even though the population increased by 10 million and the economy grew substantially.[6] Indeed, the labor participation rate is currently at 62.5% (and dropping), which is at its lowest rate since 1978, and well below the peak in 2000.

Correspondingly, economists such as Thomas Piketty, have shown conclusively that the returns on capital now exceed greatly the returns on labor.[7] The reason for that disparity is that, since the advent of integrated circuits, the productivity gains – which had fueled the rise of the middle class in America after World War II – now fuels the owners of the capital, namely the owners of the machines that have been used to increase productivity so dramatically in the last 30 years.

In short, the tools that made a worker more productive in 1958 are now *replacing* those workers entirely. Moreover, the network effect – itself a product of that same technology – has enabled those workers to be replaced on a mammoth scale. Such is the difference in capability between 1958 and today.

In the past, a few of those displaced from factory work sought opportunity in the professions that required analytical thinking. The hope was that the knowledge professions would be difficult to automate. Unfortunately, the last ten years have shown that it is the knowledge professions (such as law) which are automated most easily.[8]

Several months ago, I attended the International Legal Technology Association conference in Las Vegas, Nevada. While at this event, I attended a session hosted by IBM. The session was about IBM's use of its Watson technology and how it could be applied to the practice of law. Watson, as you may know, is the name given to an artificial intelligence program that has been in development at IBM for many years. The original Watson was used (famously) to win at the

[5] Jaron Lanier, WHO OWNS THE FUTURE? (Simon & Schuster, 2013). Jaron Zepel Lanier is an American computer philosophy writer, computer scientist, visual artist, and composer of classical music. His website is at http://www.jaronlanier.com/

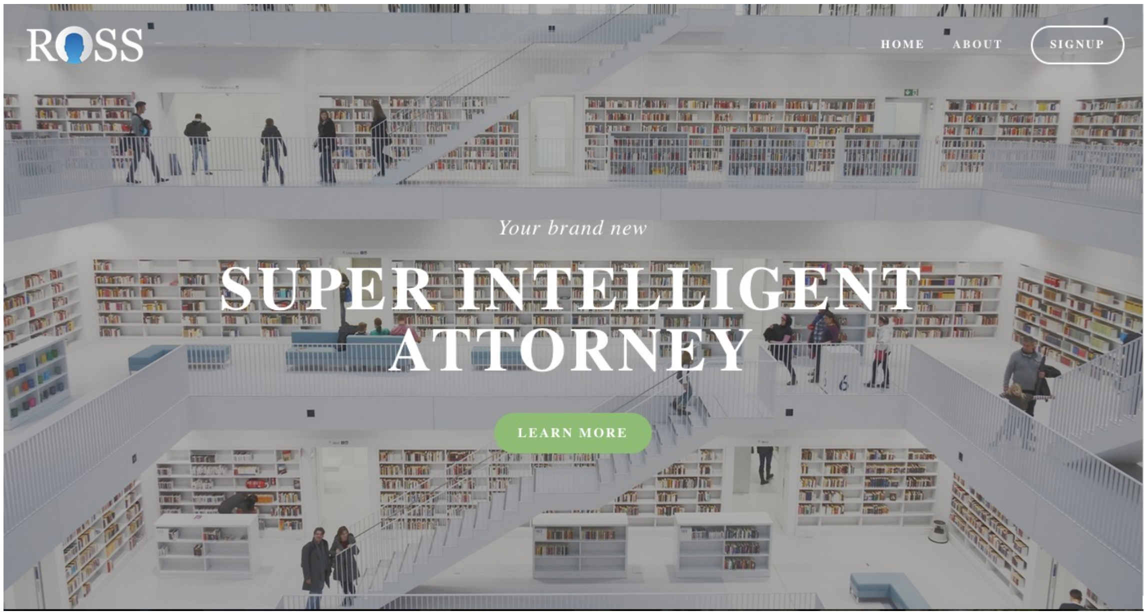
[6] *Ibid*. citing Neil Irwin, "Aughts Were a Lost Decade for U.S. Economy, Workers," *Washington Post*, January 2, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/AR2010010101196.html

[7] See, Thomas Piketty, CAPITAL IN THE TWENTY-FIRST CENTURY (2013).

[8] Ford, supra, Chapters 2-3.

TV game of Jeopardy. It has since been retired, and for all we know, is dreaming of electric sheep.

Now, however, updated versions of Watson have been developed and tailored to the practice of law. The application is called "ROSS."[9] IBM is trying to license copies of ROSS to law firms, and in particular to partners of large law firms. The idea is that ROSS can replace a human associate *entirely*. I'm not sure of the pricing scheme that IBM proposes, but it's a safe bet that it is less than the cost of a human associate. What makes ROSS particularly attractive is that doesn't require health care, doesn't eat, doesn't sleep, happily works weekends and holidays, and doesn't conspire to steal your clients. Oh, and in 18 months, it will get a new CPU that is twice as fast as the old one, thanks to Moore's law.



Your brand new
SUPER INTELLIGENT ATTORNEY

IBM touts ROSS for document review (because over 90% of documents are in electronic form). However, IBM says ROSS can do more. For instance, given a subject, Ross can go out onto the Internet and find – on its own – cases relevant to that particular topic and compare and contrast the different cases and come to its own conclusions. ROSS can also, on a daily basis, find legal news relevant to the owner's practice and inform them accordingly. Most importantly, ROSS can *learn on its own accord*. Eventually, we can expect ROSS to be able to

[9] The home page for Ross can be found at: http://www.rossintelligence.com/. At the front of that home page, Ross is touted as "Your Brand New Super Intelligent Attorney." On that website, IBM states that "ROSS is an artificially intelligent attorney to help you power through legal research. ROSS improves upon existing alternatives by actually understanding your questions in natural sentences like – 'Can a bankrupt company still conduct business?' ROSS then provides you an instant answer with citations and suggests highly topical readings from a variety of content sources."

draft to find all the business agreements on a particular topic, and draft its own tailored version based upon a term sheet.

If that wasn't bad enough, consider if all the copies of ROSS were fitted with a “phone home” feature that recorded what the licensee-attorney did with ROSS, and then describe what the attorney subsequently did for her client. What can ROSS tell its central authority? Couldn’t ROSS use the information that it has learned to mimic the ability of the partner who licensed ROSS from IBM? Could that information then be used automate the abilities of the licensee? Could then IBM then try to sell an attorney-enhanced version of ROSS to her own client?

The implications for the legal profession are obvious. Right now, this very minute, jobs in the legal profession are being automated out of existence. While you may relish the idea that attorneys in India and New Zealand are now too expensive compared to a robot, that fact does nothing for you. Associates are being automated, but in the very near future, most partners and in-house lawyers will be automated out of a job too.

IBM clearly understands the implications of their technology. They are quick to point out that, currently, ROSS is only a tool to “enhance” the work of the attorney who has licensed the technology. That’s fine if you’re the partner and not the newly minted lawyer coming out of law school with a crushing debt load. IBM is right; there will still be lawyers 20 years from now. What IBM doesn’t care to admit is that there will be far fewer lawyers then than now.

In their seminal work on the future of professions, Richard Susskind and Daniel Susskind[10]focused on “doctors, lawyers, teachers, accountants tax advisers, management consultants, architects, journalists, and the clergy (amongst others), on the organizations in which they work, and the institutions that govern their conduct.”[11] In that book, they claimed that:

> “[W]e are on the brink of a period of fundamental and irreversible change in the way that the expertise of these specialists is made available in society. Technology will be the main driver of this change. And, in the long run, we will neither need nor want professionals to work in the way that they did in the twentieth century and before.”[12]

[10] Richard Susskind and Daniel Susskind, THE FUTURE OF THE PROFESSIONS: HOW TECHNOLOGY WILL TRANSFORM THE WORK OF HUMAN EXPERTS (Oxford University Press, 2015).

[11] *Ibid*. at 1.

[12] *Ibid*.

Broader Implications for Society

The professions occupy a special place in society. Indeed, it is that special status that requires the professionals to act ethically, both for their clients and for society as a whole. However, the justification for that “grand bargain” is being undermined.[13] When the ability to know and manipulate knowledge is within the grasp of the average individual, the need for professionals is eliminated. Unfortunately, it is not clear what those professionals are going to do. Or for that matter, what will happen to our economic system when the current trend of automation reaches its logical conclusion?

What happens when software offers abundance – but only when you can afford it – is the focus of Lanier's book. As “Big Data” learns more about us, the corporations that wield it will be in a better position to strike increasingly harder bargains with consumers – and what will happen in the Capitalist-centric America when most of the citizens have no money? Stephen Hawking summed up the problem succinctly:

> “If machines produce everything we need, the outcome will depend on how things are distributed. Everyone can enjoy a life of luxurious leisure if the machine-produced wealth is shared, or most people can end up miserably poor if the machine-owners successfully lobby against wealth redistribution. So far, the trend seems to be toward the second option, with technology driving ever-increasing inequality.”[14]

Kurt Vonnegut saw this problem coming decades ago. In his 1952 novel “Player Piano,” one of the main characters quipped:

> “If you compete with a slave, you *are* a slave.”[15]

[13] *Ibid* at 9-45.

[14] Alexander C. Kaufman, “Stephen Hawking Says We Should Really Be Scared Of Capitalism, Not Robots,” Huffington Business (October 8, 2015), available at http://www.huffingtonpost.com/entry/stephen-hawking-capitalism-robots_5616c20ce4b0dbb8000d9f15

[15] Kurt Vonnegut, Jr., PLAYER PIANO (1952).

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.

Return to Table of Contents

Speculative Data Breach Damages Might Be Actionable

Whether a "risk of future harm" is sufficient for standing in data breach cases depends on whom you ask.

By: Pierre Grosdidier

Class action lawsuits naturally follow data breaches in which hackers penetrate a company's network and steal consumers' or employees' Personally Identifiable Information ("PII") *en masse*, especially when the network is a retailer's payment system. In these cases, plaintiffs allege various causes of action including claims for the substantial or increased risk of future harm because of the breach ("future harm" claims). But not all courts allow these claims to proceed without more. Courts usually dismiss future harm claims for lack of standing when plaintiffs cannot show that the breach has already resulted in tangible injury. Conversely, courts usually deny motions to dismiss when plaintiffs allege that some injury has already occurred. The Federal Trade Commission ("FTC") asserts that the FTC Act's Section 5 (15 U.S.C. § 45) authorizes it to proceed against companies whose security practices placed PII at risk even in the complete absence of tangible consumer injury. This article illustrates these three possible outcomes with recent judicial decisions and pleadings. Counsel for companies who are victims of a data breach should look closely at the facts both before and after the breach to analyze the merits of future harm claims from plaintiffs and from the FTC.

A plaintiff in federal court must have "standing" or capacity to sue. A plaintiff has standing if it can show (1) an injury in fact; (2) causation between the defendant's conduct and the injury; and (3) the likelihood that prevailing in court will redress the alleged injury.[1] The U.S. Supreme Court held in *Clapper v. Amnesty Int'l USA* that to satisfy the first standing element, the injury must be "concrete, particularized, and actual or imminent."[2] "Allegations of possible future injury" are insufficient, as are allegations that are too speculative. The "threatened injury must be *certainly impending* to constitute injury in fact, and . . . [a]llegations of *possible* future injury are not sufficient."[3] A federal court does not have subject-matter jurisdiction unless the plaintiff has standing.

[1] *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992).

[2] 568 U.S. –––, 133 S.Ct. 1138, 1147 (2013).

[3] *Id.* (internal citations omitted) (emphases in original).

Return to Table of Contents

Most courts deny standing to data breach plaintiffs in the absence of present tangible injury. Courts generally deny standing to consumer victims of data breaches who allege future harm claims but cannot demonstrate a past or present injury-in-fact. In *Reilly v. Ceridian Corp.*, for example, defendant Ceridian suffered a breach but the extent of the data theft was unknown. The court held that "allegations of hypothetical, future injuries do not establish standing under Article III."[4]

More recently, in *In re SuperValu, Inc.*, a federal district court dismissed for lack of standing a class action by 16 consumers allegedly injured by a data breach at a retail grocery chain.[5] Only one plaintiff had suffered a tangible injury from a lone fraudulent credit card transaction, and this plaintiff did not even claim that the card issuer refused to bear the loss. Nonetheless, they alleged, *inter alia*, that they faced a "substantial risk of future harm" from the loss of their PII.

The court agreed with the defendants that the plaintiffs' future harm allegations were too speculative to satisfy Article III standing. Citing *Reilly and* several post-*Clapper* cases, the court followed the "vast majority of courts" that have found insufficient harm to grant standing to plaintiffs when their stolen PII has not been misused. In this case, the breach affected over 1,000 retail stores, but even though a year and a half had passed since the breach, the plaintiffs could only complain of one fraudulent transaction. This lone transaction, the court found, was not even necessarily tied to the breach. Thus, the court could only speculate as to the true extent of the breach, i.e., whether the hackers actually captured any PII and intended to use it. For these reasons, the court held that the plaintiffs' future harm allegations did not meet Article III's standing threshold, and it dismissed the claim without prejudice.

Some courts denying standing for future harm claims in data breach cases also stress that the passing of time undercuts the plaintiffs' argument. In *Whalen v. Michael Stores Inc.*, for example, the court adopted other courts' dicta that the passing of time after a breach without a showing of harm "undermines any argument that the threat of that harm is immediate, impending, or otherwise substantial."[6] In that case, Whalen had not incurred any fraudulent charges almost two years after the breach.

[4] 664 F.3d 38, 41 (3d Cir. 2011).

[5] No. 14-MD-2586, 2016 WL 81792 (D. Minn. Jan. 7, 2016).

[6] No. 14-CV-7006, --- F. Supp. 3d ---, 2015 WL 9462108, at *5 (E.D.N.Y. Dec. 28, 2015) (citing cases).

Return to Table of Contents

Other courts grant standing when plaintiffs have suffered a tangible injury.

Courts have found standing for data breach plaintiffs for future harm claims when an actual injury has already occurred. In *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit Court of Appeals reversed a district court that had dismissed consumers' future harm claims for lack of standing.[7] Hackers stole some 350,000 credit card numbers from Neiman Marcus, and 9,200 cards were used illicitly after the breach. Two of the plaintiffs were compensated for unauthorized charges. The court rejected defendant's argument that plaintiffs' future harm claims were too speculative and barred by *Clapper*. The court found that the data breach's factual record showed that the risk that hackers would misuse the captured data was "immediate and very real."[8] There was "no need to speculate" whether and what information was stolen. Injury from the data theft was not speculative but "objectively reasonabl[y] likel[y]," and consumers "should not have to wait" to be injured to gain standing. The court found plaintiffs' allegations of future harm "plausible," and held that they were "sufficient to survive a [Rule] 12(b)(1) motion" to dismiss for lack of subject matter jurisdiction.

Likewise, in *Corona v. Sony Pictures Entm't, Inc.*, employees sued Sony after their PII was stolen during a data breach.[9] The employees alleged that the PII was posted on Internet sites for use by identity thieves, and that some employees and their families had received emails containing threats of physical harm. The court held that these allegations of future harm were sufficiently immediate and impending to justify plaintiffs' standing to sue.

The FTC asserts that it can file a Section 5 complaint even in the absence of an actual data breach and its attendant consumer injury.

The FTC argues that the injury-in-fact component of the Article III standing test does not apply to an FTC complaint. Section 5 of the FTC Act bars "unfair or deceptive acts or practices in or affecting commerce" and authorizes the FTC to police such conduct.[10] But the FTC's authority is restricted to acts that, *inter alia*, cause or are "likely to cause substantial injury to consumers."[11] In *In re LabMD, Inc.*, the FTC took the position that a company's lax computer

[7] 794 F.3d 688, 690-91 (2015).

[8] *Id.* at 693 (*citing In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) (Koh, J.)); *but see In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617, --- F. Supp. 3d ---, 2016 WL 589760, at **23-26 (N.D. Cal. Feb. 14, 2016) (Koh, J.) (holding that "Imminent Risk of Further Costs" is not a cognizable injury under New York's General Business Law § 349 in data breach class action where one plaintiff was allegedly victim of a false filed tax return).

[9] No. 14-cv-09600, 2015 WL 3916744, at *1 (C.D. Cal. June 15, 2015).

[10] 15 U.S.C. § 45(a)(1)-(2).

[11] *Id.* § 45(n).

Return to Table of Contents

security measures are actionable under the FTC Act when they pose a significant risk of concrete harm via a data breach and are likely to cause substantial consumer injury. According to the FTC, proof of an actual data breach is not required.[12] The FTC relied on a footnote in its 1980 Policy Statement to support its position.[13] This footnote stated that "[a]n injury may be sufficiently substantial," and fall within Section 5's ambit, "if it raises a significant risk of concrete harm." Under this argument, Section 5 liability can be imposed merely based on the risk that inadequate security measures will cause a data breach resulting in future consumer harm. Significantly, the FTC's Appeal Brief did not offer uncontroverted case law to support its position, a shortcoming that LabMD highlighted in its response brief.[14] In its recently-filed Reply Brief, however, the FTC belatedly cited the Third Circuit's *FTC v. Wyndham Worldwide Corp.* decision, which noted that the FTCA's § 45(n) "expressly contemplates the possibility that conduct can be unfair before actual injury occurs."[15] The Reply Brief also cited to an unreported 2014 injunctive order issued by a district court in a case where the Commission did not allege actual misuse of consumer information, but with facts substantially different from those in *In re LabMD*.[16]

The factual and procedural histories of the FTC's complaint against LabMD are complicated and controversial. LabMD was a Georgia medical testing company founded in 1996.[17] The FTC filed a complaint against LabMD in 2013 after a third-party, Tiversa, Inc., found a PII-containing file (the "1718 File") on a LabMD computer folder in 2008, which was accessible via Internet through peer-to-peer software. Tiversa turned over the 1718 File to the FTC under circumstances that led to a congressional inquiry and ultimately to what an amicus described

[12] Complaint Counsel's Appeal Brief, *In re LabMD, Inc.*, FTC No. 9357, at 5□7, 10□12 (Dec. 22, 2015) ("Appeal Brief"). The *In re LabMD* pleadings are available at https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[13] *Id*. at 12 (*citing* Letter from FTC to Senators Ford and Danforth (Dec. 17, 1980), reprinted in H.R. REP. No. 156, Pt. 1, 98th Cong., 1st Sess. 33, 36 n.12 (1983) ("1980 Policy Statement")).

[14] Respondent LabMD, Inc.'s Corrected Answering Brief, FTC No. 9357, at 2-3 (Feb. 5, 2016) ("Answering Brief").

[15] Complaint Counsel's Reply Brief to Respondent's Answering Brief, FTC No. 9357, at 11 (Feb. 23, 2016) ("Reply Brief") (citing FTC v. Wyndham Worldwide Corp., 799 F.3d, 236, 246 (3d Cir. 2015)).

[16] *FTC v. Cornerstone & Co., LLC*, No. 1:14-CV-01479 (D.D.C. Sept. 10, 2014) (Order for Entry of Preliminary Injunction), available at https://www.ftc.gov/system/files/documents/cases/141001cornerstoneorder.pdf.

[17] *See* Initial Decision, *In re LabMD, Inc.*, FTC No. 9357, at 18 (Nov. 13, 2015) ("Initial Decision").

Return to Table of Contents

as a “devastating report” for both the FTC and Tiversa.[18] LabMD eventually unwound its operations in 2014.

In its Initial Decision dismissing the FTC’s complaint, the Administrative Law Judge (“ALJ”) found, *inter alia*, that there was no evidence that the 1718 File was downloaded by anyone other than Tiversa, or that anyone named in the 1718 File was harmed after more than *seven years* had passed since the its exposure on Internet.[19] The ALJ held that “Complaint Counsel ha[d] proven the ‘possibility’ of harm, but not any ‘probability’ or likelihood of harm.”[20] The ALJ specifically rejected the FTC’s argument that Section 5 liability can be imposed solely on the basis of the risk of a data breach. Citing *Reilly*, the ALJ reasoned that to conclude that the consumers whose PII was kept on LabMD’s computer network were likely to suffer future harm “would require speculation upon speculation.” The ALJ also pointed to the FTC’s 1980 Policy Statement and 1982 Policy Letter, both stating that the FTC should concern itself with “substantial” injuries, and not “trivial or merely speculative harm.”[21]

In its Appeal Brief, the FTC rejected the Initial Decision’s reliance on *Reilly*, calling it “misplaced.”[22] Unlike Article III standing, the FTC argued, Section 5(n) does not require injury-in-fact. Instead, a “significant risk of concrete injury” allegedly constitutes, in and of itself, “substantial injury.” Moreover, it also argued that Congress granted the FTC standing to enforce Section 5, and a private party’s Article III standing analysis in a judicial data breach proceeding is irrelevant to an FTC enforcement action. But as LabMD pointed out, the case law contains “no decision or binding precedent where a respondent was found to have violated Section 5(n) based only on allegations regarding possible risk of likely substantial harm.”[23]

[18] Proposed Amicus Curiae Brief of TechFreedom in support of the Position of Respondent Counsel, *In re LabMD, Inc.*, FTC No. 9357, at 4 (Feb. 5, 2016) (*citing Tiversa, Inc.: White Knight or Hi-Tech Protection Racket?*, Comm. on Oversight and Gov’t Reform, U.S. House of Rep., 113th Cong. (Jan. 2, 2015)) (“Committee Report”).

[19] Initial Decision, at 60, 64.

[20] *Id*. at 14.

[21] 1980 Policy Statement, *supra* note 14, at 36; Letter from FTC Chairman J.C. Miller, III to Senator Packwood and Senator Kasten (March 5, 1982), reprinted in H.R. REP. No. 156, Pt. 1, 98th Cong., 1st Sess. 27, 32 (1983) (“1982 Policy Letter”).

[22] Appeal Brief, *supra* note 13, at 21.

[23] Answering Brief, *supra* note 15, at 3. The *Cornerstone* Stipulated Final Order for Permanent Injunction does not contain a finding of guilt by the defendants, who “neither admit nor deny any of the allegations in the Complaint.”

Return to Table of Contents

Both the ALJ's Initial Decision and the FTC's Appeal Brief invoke different language in the same document (the 1980 Policy Statement) to justify, in part, their positions. *In re LabMD* is now on appeal to the full Commission. The stakes are high for the FTC after the critical Committee Report, and even the Commission's decision might not spell the end of this proceeding and its attendant controversy.

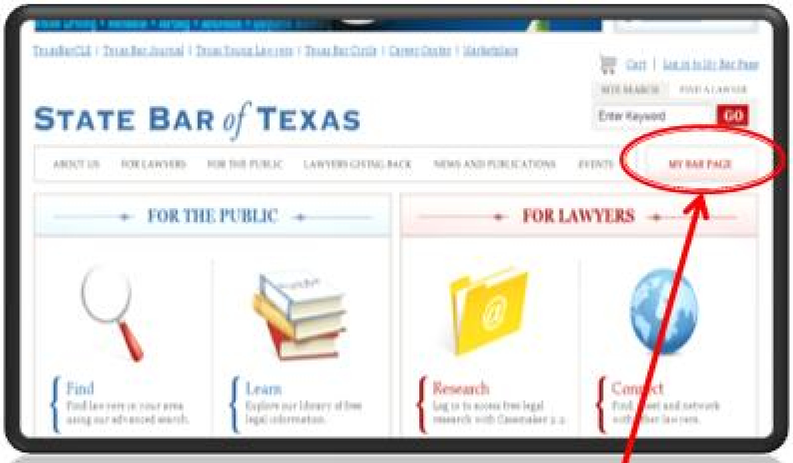
About the Author:

Pierre Grosdidier is an Attorney in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. His practice focuses on complex commercial litigation, especially lawsuits and arbitrations with strong technical elements. He has litigated cases involving the Computer Fraud and Abuse Act and the stored Communications Act, and also trade secret, construction, oil and gas, and software copyright claims. Pierre is also a member of Haynes and Boone's Privacy and Data Breach focus group. Prior to practicing law, Pierre worked in the process control industry straddling refining, automation, and software. 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

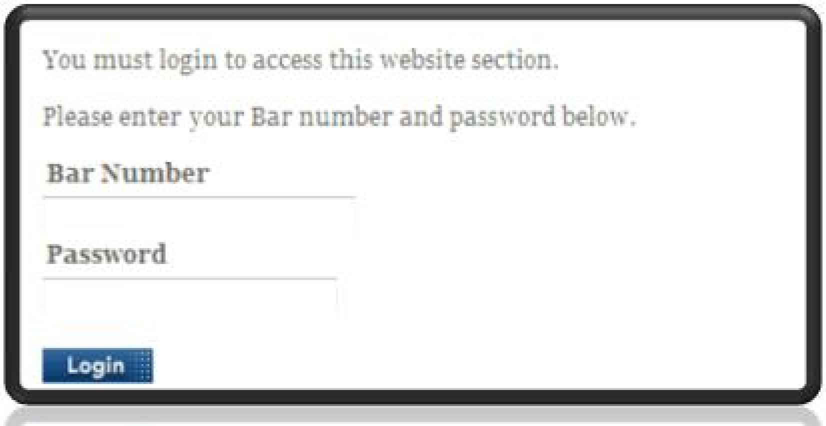
How to Join the State Bar of Texas Computer & Technology Section

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

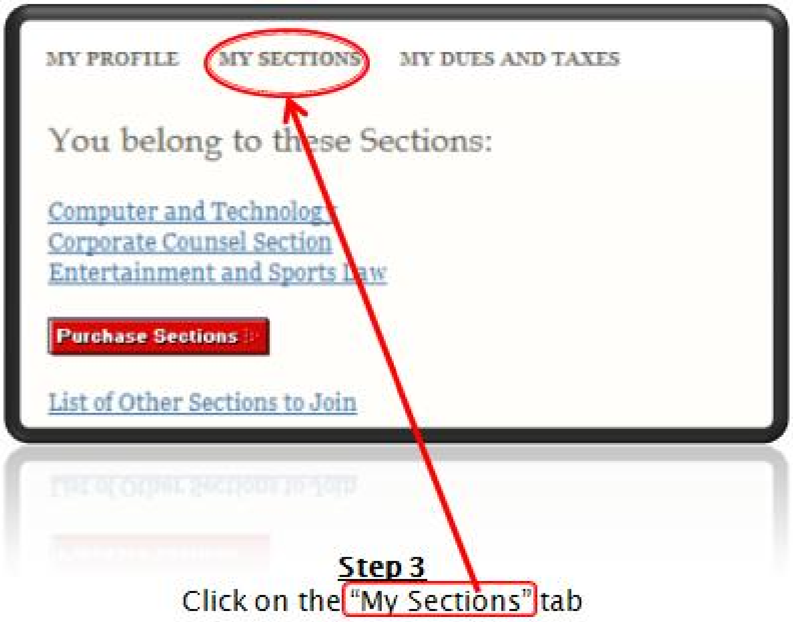
Password

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.

Return to Table of Contents

State Bar of Texas Computer & Technology Section Council

Officers

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

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

Computer and Technology

Section

Return to Table of Contents