COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas
June 2019

STATE BAR OF TEXAS
Created in 1939

SECTION LEADERSHIP

CHAIR
Sammy Ford, IV

CHAIR-ELECT
John G. Browning

TREASURER
Shawn Tuma

SECRETARY
Elizabeth Rogers

NEWSLETTER EDITORS
Pierre Grosdidier
Kristen Knauf

CLE COORDINATOR
Reginald Hirsch

IMM. PAST CHAIR
Michael Curran

COUNCIL MEMBERS
Lisa Angelo
Eddie Block
Chris Krupa Downs
Eric Griffin
Seth Jaffe
Sanjeev Kumar
Hon. Emily Miskel
Rick Robertson
Hon. Xavier Rodriguez
William Smith

CLICK ON TITLE TO JUMP TO ARTICLE

Note from the Chair by Sammy Ford

Letter from the Co-Editors by Pierre Grosdidier & Kristen Knauf

Featured Articles

- Authenticating Electronic Evidence: Texas Approach versus Maryland Approach by Judge Emily Miskel
- Block What?!? - Vermont Enacts the First Blockchain-Based LLC by Ronald Chichester
- EDPB Guidance on GDPR's Jurisdictional Scope by Thomas W. Hayde and Ben Shantz
- Where Approved Power of Attorney Forms Fail You on Digital Assets and Problems Your Clients or You May Not Anticipate by Joseph Jacobson
- California Leads the Way in IoT Security Legislation by Seth Jaffe
- The Illinois Biometric Information Privacy Act after *Rosenblach*: A Preview of What's to Come? by William Smith
- 15 Cases and Statutes in 45 Minutes by Lisa Angelo, Pierre Grosdidier, and Shawn Tuma
- Senators Introduce The DETOUR Act to Ban "Dark Patterns" on Internet by Pierre Grosdidier

Op-Eds

- Arrestee DNA Solves Crimes and Saves Lives by Jayann Sepich
- 23 and Me: Where I am in Legal Tech Competence as I Hit my 23rd Year of Practice by Mark I. Unger

Short Circuits

- Featuring Ryan Gardner, Ronald Chichester, and Seth Jaffe

CircuitBoard

- Featuring Kristen Knauf, Al Harrison, Ronald Chichester, and Pierre Grosdidier

Join our section!

Contents

Note from the Chair 4

By Sammy Ford 4

Letter from the Co-Editors 6

By Pierre Grosdidier & Kristen Knauf....................6

Featured Articles:-

Authenticating Electronic Evidence: Texas Approach versus Maryland Approach....................8

By J. Emily Miskel 8

About the Author 10

Block What?!? – Vermont Enacts the First Blockchain-Based LLC....................11

By Ronald Chichester....................11

About the Author 17

EDPB Guidance on GDPR's Jurisdictional Scope 18

By Thomas W. Hayde and Ben Shantz 18

About the Authors....................20

Where approved Power of Attorney forms fail you on Digital Assets and problems your clients or you may not anticipate.....................22

By Joseph Jacobson 22

About the Author 32

California Leads the Way in IoT Security Legislation 33

By Seth Jaffe....................33

About the Author 36

The Illinois Biometric Information Privacy Act after *Rosenbach*: A Preview of What's to Come?....................37

By William Smith....................37

About the Author 43

15 Cases and Statutes in 45 Minutes 44

By Lisa Angelo, Pierre Grosdidier, Shawn Tuma 44

About the Authors....................49

Senators Introduce The DETOUR Act to Ban “Dark Patterns” on Internet 51
By Pierre Grosdidier 51
About the Author 53

Op-Eds:-

Arrestee DNA Solves Crimes and Saves Lives 54
By Jayann Sepich 54
About the Author 57

23 and Me: Where I am in Legal Tech Competence as I Hit my 23rd Year of Practice 58
By Mark I. Unger 58
About the Author 60

Short Circuits:-

Space: The Final Frontier of Government Regulation 61
By Ryan Gardner 61
About the Author 62

LinkNYC: What Sounds Like a Great Idea Can Have Some Serious Downsides 63
By Ronald Chichester 63
About the Author 64

Beware of Puffery in Your Security Representations 65
By Seth Jaffe 65
About the Author 66

CircuitBoards:-

re:SearchTX Gives Users Access to All Civil Lawsuit Filings in all 254 Texas Counties From a Single Portal 67
By Kristen Knauf 67
About the Author 68

A few of my favorite and most useful regularly used apps invoked on my Android Samsung S7 Edge: 69
By Al Harrison 69
About the Author 71

What is an Aggregator? And Why Do Some Attorneys Find Them Essential? 72
By Ronald Chichester and Lisa Angelo 72
About the Authors 80

A Lawyer's Genetic Fingerprinting Primer 81
By Pierre Grosdidier 81
About the Author 86

How to Join the State Bar of Texas Computer & Technology Section 87

State Bar of Texas Computer & Technology Section Council 89

Chairs of the Computer & Technology Section 89

Note from the Chair

By Sammy Ford

It is bittersweet writing this, my last introduction to *Circuits* as Chair of the Computer & Technology Section. I believe we have accomplished so much and continue to serve as a valuable resource to the members of the section in particular and our bar in general.

Even though I have spent the past few issues writing about the particular benefits that this Section provides to its members, I would be remiss to not point out how the Section's members in particular provide benefit to the bar at large. In the most recent issue of the Texas Bar Journal (May 2019) three members of our Section's Council wrote articles. Elizabeth Rogers wrote on the new duty of technical competence added by the Supreme Court shortly before we went to press with the last issue of *Circuits*. Mark Unger provided the bar-at-large with a report from the ABA's annual TECHSHOW, which I discussed in earlier issues. Finally, our incoming Chair, John Browning, wrote a humorous piece, demonstrating our members' versatility. These contributions follow Pierre Grosdidier's April 2019 technology column, where he highlighted the possible challenges to suing providers of custom-designed software in light of Texas's Certificate of Merit Statute.

I'd also like to report that members of our Council recently met with members of the United States Court of Appeals for the Fifth Circuit's technology department for an in-depth look at some of the new technology that will be available to practitioners in that Court and the technology in use by the Judges themselves. Already the Court provides real time proofing of briefs to make sure they comply with local rules (would that all courts do that) and soon Pacer will automatically detect the filing that a lawyer is making and also provide deadlines for various filings. Cool stuff!

In other news, San Francisco recently became the first city to ban the use of facial recognition technology by the police and the government generally. The ban does not apply to private businesses or the federal government. The ban is the first in what I expect will be numerous attempts to come to grips with the fast moving, and somewhat uncertain future of artificial intelligence. Even though our Section will not take any position on this or any other particular policy, we will continue to be at the forefront of analyzing the legal ramifications of new technologies like artificial intelligence in general and its particular applications.

Finally, I would like to take a moment and recognize Pierre Grosdidier for the work that he has done in greatly expanding *Circuits* during this bar year. It was my goal to increase both the quantity and quality of information that we provided to our members. And I believe we accomplished that.

COMPUTER AND
TECHNOLOGY
SECTION

Letter from the Co-Editors

By Pierre Grosdidier & Kristen Knauf

Welcome to the fourth and final issue of *Circuits* for the 2018-19 bar year. What a year it has been for *Circuits*, and what a final issue we have for you! Every legal specialization is unique, challenging, and evolving in its own ways. But, ours (computer and technology law) probably beats the others in how rapidly it evolves and how frequently new, deep, and important issues arise because technology changes and everyday engineers think of novel ways to surprise us. What better way to keep up with all these legal developments and issues than to be a member of our section and read *Circuits*? We hope that you will have time to read and enjoy all the articles in this final 2018-19 issue of our Section eJournal, and we thank you for your participation in the Computer & Technology Section. Please spread the word that we have great things going on.

In our *Feature Articles*, we start with a contribution from Judge Emily Miskel, who compares the standards of authentication of electronic evidence between Texas and Maryland. Ronald Chichester, past-Section Chair, next introduces us to Blockchain-based LLC, a new form of business entity recognized by Vermont. Guest Contributors Thomas Hayde and Ben Shantz discuss European Board of Data Protection guidance regarding the territorial scope of the GDPR. Joseph Jacobson, past-Section Chair, introduces us to the Texas Revised Uniform Fiduciary Access to Digital Assets Act, and highlights some of the knotty issues that it raises. Seth Jaffe, current Council Member, discussed California's recent Internet of Things statute. His colleague William Smith does the same with Illinois' Biometric Information Privacy Act. Finally, Lisa Angelo (current Council Member), yours truly (Pierre Grosdidier), and Shawn Tuma (Current Treasurer) summarize their "15 statutes and cases in 45 Minutes" presentation, which they will panel at this year's Annual Bar Conference.

Next, we welcome two op-eds from Jayann Sepich and Mark Unger. Ms. Sepich is the co-founder of *DNA Saves*, a non-profit organization that advocates for arrestee DNA legislation. She has lobbied in favor of passing Texas HB-1399, a law that would broaden the category of arrestees whose DNA is automatically tested. The Texas House and Senate sent this bill to the Governor on May 29, 2019. A companion *CircuitBoard* titled "A lawyer's genetic fingerprinting primer" will tell interested readers all they need to know about DNA testing. Separately, our past-Section Chair Mark Unger muses on the rapid evolution of technology and the duty—and the necessity—of remaining technically competent. Of course, the opinions expressed in these op-eds are those of their authors and not those of the Computer & Technology Section, the State Bar of Texas, and their respective officers.

In our *Short Circuits*, guest author Ryan Gardner explains why not just anyone can send a satellite into space (amateur rocketeers beware). Ron Chichester tells us what happened when the City of New York decided it would give all its denizens access to Internet without working out all the privacy issues first. And, Seth Jaffe explains that too much puffery in a company's security representations can draw the attention of the Federal Trade Commission.

Finally, in *CircuitBoards*, yours truly (Kristen Knauf) talks about how re:SearchTX makes all state court filings in all 254 Texas counties easily available online. Ronald Chichester and Lisa Angelo explain how aggregators can help you stay abreast of all new legal developments. Pierre Grosdidier explains how genetic fingerprinting works, without requiring you to pull out that senior high-school biology book of yours stored in a box somewhere in your parents' garage. And, past-Chair Al Harrison shares with us four of his favorite apps, which he uses to run his law practice effectively and securely.

Many thanks to all the contributors to this new issue and for helping us keep this publication on schedule. Thank you also to Antony P. Ng for his review of and assistance with this issue's articles. We hope that you enjoy this new edition of *Circuits* and, as always, we welcome any comments or submissions that you may have: please send them to our section administrator at admin@sbot.org.

Kind Regards,

Pierre Grosdidier, Co-Editor

Kristen Knauf, Co-Editor

FEATURED ARTICLES:-

Authenticating Electronic Evidence: Texas Approach versus Maryland Approach

By J. Emily Miskel

In our legal system, judges usually function as the initial gatekeepers of whether or not a piece of evidence should be admitted based on its reliability, and juries assess the weight and credibility of admitted evidence. The test for authenticating and admitting electronic evidence is whether the proponent of the evidence has offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is. The court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so.

Jurisdictions differ as to how high this authentication hurdle is. This article will discuss the two more popular approaches—the skeptical Maryland approach and the more lenient Texas approach.

The Skeptical Maryland Approach

In *Griffin v. State*, 19 A.3d 415 (Md. 2011), the Maryland Court of Appeals (Maryland's highest court), addressed the authentication of a printout of a MySpace page. The opinion emphasized the anonymity of online sites and the ease with which anyone can create fictitious accounts. The Maryland approach is skeptical of social media and carries almost a presumption that information on the Internet is inherently untrustworthy. The *Griffin* court held that the potential for abuse and manipulation of a social networking site requires a greater degree of scrutiny. The *Griffin* court required witness testimony that closely linked the creator to the content, putting an increased burden on the proponent of the evidence to affirmatively demonstrate that the evidence is not fake. States that have adopted the Maryland approach include Colorado, Connecticut, and Mississippi.

The More Lenient Texas Approach

In *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012), the Texas Court of Criminal Appeals also addressed the authentication of a MySpace page. Under the Texas approach, a social media exhibit can be admitted based on circumstantial evidence, taken as a whole, that could support a finding by a rational jury that the exhibit was created by the party. The burden then shifts to the opponent of the evidence, after it is admitted, to challenge the weight and credibility of the exhibit by offering evidence that it is fake. Under the Texas approach, the evidence is more likely to be admitted and to be evaluated by the ultimate fact-finder. Another state has emphasized that the same uncertainties exist with traditional written documents—signatures can be forged, letterhead copied or stolen. Under the Texas approach, electronic evidence is not held to a standard higher than any other kind of evidence, and it should be evaluated under the traditional rules. States that have adopted the Texas approach include Delaware, Tennessee, Ohio, Georgia, Kansas, Massachusetts, and Missouri.

Federal Courts

Following the foundational case of *Lorraine v. Markel American Insurance Co*, 241 F.R.D. 534 (D. Md. 2007) (ironically from a federal court in Maryland), federal courts have emphasized that traditional notions of admissibility should apply to electronic evidence, and that judges should not be excessively skeptical of online evidence. The United States Court of Appeals for the Second, Fifth, Tenth, and Eleventh Circuits have upheld the authentication of evidence under a lenient standard that is similar to the Texas approach.

Example Predicate for Social Media and Internet Sites

The Texas approach to authentication permits a website exhibit to be admitted solely through testimony that it is an accurate copy of something from the Internet. Under the Maryland approach, additional testimony must be offered to link it to the purported creator. In a Texas case addressing the authentication of an online personal ad, the court held witness testimony that the exhibit was an accurate copy of an online posting was sufficient—whether the party placed the ad did not go to the authenticity of the exhibit, but, rather, to the underlying issues in the case. The Maryland approach would additionally require that a witness have personal knowledge of distinctive characteristics linking the online personal ad to its creator.

Best Practices

Courts that apply the Maryland approach are cautious that evidence obtained from the Internet can be easily faked. However, courts that apply the Texas approach respect the jury as the ultimate arbiter of authenticity.

Even if your jurisdiction follows the Texas approach, you may draw a judge who is skeptical of electronic evidence. The best practice for ensuring admissibility of social media or Internet evidence is for the sponsoring witness to testify to three elements:

(1) What was actually on the website?
(2) Does the exhibit or testimony accurately reflect it?
(3) If so, what distinctive characteristics show that it is attributable to the party?

About the Author

Judge Emily Miskel of the 470th district court of Collin County, Texas is board certified in family law by the Texas Board of Legal Specialization. Judge Miskel has an engineering degree from Stanford University, and she received her law degree from Harvard Law School. Before she was judge of the 470th district court, she practiced family law in Plano, Texas.

Block What?!? – Vermont Enacts the First Blockchain-Based LLC

By Ronald Chichester

I. Introduction

In 2018, Vermont enacted a bill to modify its Title 11 (Corporations, Partnerships and Associations) by adding subchapter 12 to Chapter 25 (the part of the law that enables the creation of limited liability companies ("LLCs")). The new subchapter 12 is devoted specifically to blockchains, and enables the formation of a new type of corporation, the blockchain-based LLC ("BBLLC").[1] This article will discuss the elements of subchapter 12, and give a very brief introduction to blockchains.

II. What is a Blockchain?

The Securities and Exchange Commission ("SEC") provides a brief introduction to blockchains specifically for lawyers.[2] In a nutshell, a blockchain is a ledger that, depending upon its design, can serve as an alternate trust mechanism that differs significantly from the "traditional" trust mechanism that is familiar to all lawyers. In the traditional trust paradigm, the identity of the parties is generally known, but what transpires between them can be murky. In the traditional paradigm, jurisdiction is fundamental, and the rules of procedure and evidence are geared toward clarifying what acts took place between the parties. In stark contrast, the blockchain trust paradigm does not even attempt to identify the parties. What transpires between the parties, however, is known precisely because each act is recorded indelibly on the blockchain. Because the acts between the parties are known with complete precision, the blockchain trust paradigm can dispense with certain requirements necessary to the traditional paradigm (such as the identity of the parties).

Because blockchains are implemented on computers that are connected to a network, they facilitate the automation of business processes—and it is the automation of business processes that has led to the creation of new types of corporate business models and thus

[1] *See,* 11 V.S.A. §§ 4171-4176.

[2] *See,* Nancy Liao, "A Brief Introduction to Blockchain," available at: https://www.sec.gov/spotlight/investor-advisory-committee-2012/slides-nancy-liao-brief-intro-to-blockchain-iac-101217.pdf. For a more in-depth review of blockchains and the trust-paradigms, *see* KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST (2018). *See also,* 'Blockchain Law Class: 01 Introduction," available at: https://www.blockchainlawclass.com/a-brief-introduction-to-the-course-blockchain-cryptocurrency-and-law.

corporate structures. One of the most important new business models employs contract compliance on the blockchain, namely *smart contracts*.

Smart contracts utilize software to automate the performance and/or compliance of contracts between two or more parties.[3] Blockchains are central to smart contracts because the blockchain can record the activities associated with the contract, and they also are the mechanism of choice to handle the consideration.

As one theory of corporations is a nexus of contracts,[4] is it possible to have a nexus of smart contracts to make a "smart corporation?" The answer to that question is "yes," and those entities are called various things, most commonly a "decentralized autonomous organization" or "DAO."[5] While DAOs are an engaging topic, it is beyond the scope of this article because the Vermont statute does not facilitate DAOs.

Both smart contracts and DAOs provide sufficient motivation for corporations to adopt blockchains. However, blockchains also enable corporations to create their own digital currency, which can streamline operations with vendors and reduce bank fees and attendant financial lags induced by the current banking structure.[6]

[3] For a brief introduction to smart contracts (tailored to lawyers), *see*, *e.g.*, "What are Smart Contracts," available at: https://blockgeeks.com/guides/smart-contracts/.

[4] For a brief introduction to the nexus theory of contracts to define a corporation, *see, e.g.,* Academike, "Corporations as Nexus of Contracts: A Critique" (December 17, 2014), retrieved from https://www.lawctopus.com/academike/corporation-nexus-contracts-critique/.

[5] Decentralized Autonomous Organizations, also known as digital corporations, are corporations that exist entirely on the blockchain. Under the nexus theory of contracts, a corporation is nothing but a set of contracts. If all of the contracts that comprise the company can be smart contracts, then the entire company can exist on the blockchain—no employees, and (perhaps) no need to avail the company to a particular jurisdiction. *See*, *e.g.*, "Decentralized autonomous organizations," available at: https://en.wikipedia.org/wiki/Decentralized_autonomous_organization; William Maugayar, "An Operational Framework for Decentralized Autonomous Organizations" (Startup Management, February 4, 2015), retrieved from http://startupmanagement.org/2015/02/04/an-operational-framework-for-decentralized-autonomous-organizations/; and Blockonomi, "What is a DAO? Decentralized Autonomous Organizations & the Ethereum Hack" (July 3, 2018), retrieved from https://blockonomi.com/what-is-a-dao/.

[6] *See*, *e.g.*, Will Yakowicz, "Forget Bitcoin. These Startups Will Help Your Company Make Its Own Digital Currency," (Inc. magazine), retrieved from https://www.inc.com/will-yakowicz/forget-bitcoin-these-startups-help-you-make-your-own-currency.html; A.J. Agrawal, "How Blockchain is Streamlining Business Operations," (February 16, 2018), retrieved from https://thenextweb.com/contributors/2018/02/16/blockchain-streamlining-business-operations/.

III. Subchapter 12 – BBLLCs

Subchapter 12 covers: definitions;[7] election;[8] authority & attendant requirements;[9] multiple roles of members and managers;[10] consensus formation algorithms and governance processes;[11] and finally the scope of the subchapter in relation to other state laws.[12] While Vermont's new law can benefit companies who wish to adopt blockchains for business operations, it stops short of the needs for entirely digital corporations, namely distributed autonomous organizations.[13]

a. Definitions

There are only four definitions within subchapter 12.[14] Those who thought that they would find a working definition of blockchains in subchapter 12 might be disappointed. Blockchains are now so prevalent in law that even the definition of "blockchain technology" in subchapter 12 merely references a previous statute.[15] Two other definitions cover "protocols"[16] (not computer protocols, per se, but the regulatory model that is implemented in software for the BBLLC as a whole), and "virtual currency"[17] which can be a medium of exchange for parties dealing with the BBLLC. Virtual currency has a sensible (and common) meaning. However, protocol refers to the design of the blockchain itself. The Vermont legislature, apparently, understood that the design of the blockchain could have a substantial effect on the success of the blockchain, and

[7] 11 V.S.A. § 4171.

[8] 11 V.S.A. § 4172.

[9] 11 V.S.A. § 4173.

[10] 11 V.S.A. § 4174.

[11] 11 V.S.A. § 4175.

[12] 11 V.S.A. § 4176. The scope of the law is limited and doesn't exempt or exclude a BBLLC from any other state laws.

[13] Distributed autonomous organizations are a set of smart contracts that are interrelated to form an organization that behaves like a corporation—only without any (human) employees. Those types of organizations exist entirely on a blockchain. *See, e.g.,* DAO.EOS (http://www.daoeos.io/). They are also known as decentralized autonomous organizations and decentralized autonomous corporations. *See*, Wikipedia (https://en.wikipedia.org/wiki/Decentralized_autonomous_organization).

[14] *See,* 11 V.S.A. § 4171.

[15] Specifically, 12 V.S.A. § 1913.

[16] 11 V.S.A. § 4171(3).

[17] 11 V.S.A. § 4171(4). Virtual currencies are, by now, well known in the legal community. There are many explanatory videos and papers available on the topic, such as "Bitcoin: Your Guide To Understanding Digital Currency [Documentary]", available at: https://www.youtube.com/watch?v=SmExLsqQYEw.

its attendant vulnerabilities.[18] Consequently, as part of the process of incorporation as a BBLLC, the design of the one or more blockchains will need to be disclosed.

Far and away, however, the most important definition is that of "participant."[19] The definition of "participant" under subchapter 12 is fairly broad and encompasses three types of individuals. The first type of participant to be identified are those that have "a partial or complete copy of the decentralized consensus ledger or database utilized by the blockchain technology, or otherwise participates in the validation processes of such ledger or database."[20] The second type of participant to be identified in the incorporation process includes "each person in control of any digital asset native to the blockchain technology."[21] The third type of participant to be identified includes "each person that makes a material contribution to the protocols."[22] These participants are central to the definition of the protocols to be used by the BBLLC, and indicate that Vermont's legislature appreciated the importance of the design of the blockchain to the potential success of a BBLLC and an individual may have a significant effect on a corporation without being a manager or part-owner of the corporation. As a practical matter, it is not clear whether the incorporating company will have to disclose all of the owners of nodes[23] for the blockchain if the BBLLC elects to use a large, public blockchain such as Bitcoin. However, if there are few participants, the incorporating company will almost certainly have to disclose the identities of participants.

[18] For examples of blockchain vulnerabilities, *see*, *e.g.,* Blockchain.us, "Blockchain Vulnerabilities" (May 22, 2018), retrieved from https://blockchain.us/blockchain-vulnerabilities/; R. Martin, "5 Blockchain Security Risks and How to Reduce Them" (November 29, 2018), retrieved from https://igniteoutsourcing.com/blockchain/blockchain-security-vulnerabilities-risks/; Infosecinstitute.com, "Blockchain Vulnerabilities: Imperfections of the Perfect System" (August 7, 2018), retrieved from https://resources.infosecinstitute.com/blockchain-vulnerabilities-imperfections-of-the-perfect-system/; and W. Thornburg, "The DAO Hack and Blockchain Security Vulnerabilities" (July 8, 2018), retrieved from https://coincentral.com/blockchain-security-vulnerabilities/.

[19] 11 V.S.A. § 4171(2).

[20] 11 V.S.A. § 4171(2)(A).

[21] 11 V.S.A. § 4171(2)(B).

[22] 11 V.S.A. § 4171(2)(C).

[23] For a description of what a "node" is, *see, e.g.*, "How Nodes Work on the Blockchain" retrieved from https://www.worldcryptoindex.com/how-nodes-work/.

b. Election

The election to make an LLC a BBLLC is quite simple: merely state explicitly that the company is to be a BBLLC and satisfy all of the other requirements of an LLC under Vermont's corporation statute.[24]

c. Authority and Attendant Requirements

This part of subchapter 12 deals with whom is authorized to do what. In general, the BBLLC may "provide for its governance, in whole or in part, through blockchain technology."[25] Note, there really aren't any limits about what the blockchain could be used for. The blockchain may be used for corporate governance, as well as financial transactions (including smart contracts).

Even though you can use a blockchain for any corporate purpose, the incorporating company must "provide a summary description of the mission or purpose of the BBLLC."[26] The incorporating company must also "specify whether the decentralized consensus ledger or database utilized or enabled by the BBLLC will be fully decentralized or partially decentralized and whether such ledger or database will be fully or partially public or private, including the extent of participants' access to information and read and write permissions with respect to protocols."[27] As mentioned above, the company must disclose the design of the various blockchains that are to be used in the company's business. One of the outstanding questions is whether the BBLLC will have to amend its documents with the Secretary of State if the company elects to add a new blockchain or modify the design of the blockchain that was disclosed initially.

With respect to corporate governance, the BBLLC may "adopt voting procedures, which may include smart contracts carried out on the blockchain technology, to address: (i) proposals from managers, members, or other groups of participants in the BBLLC for upgrades or modifications to software systems or protocols, or both;[28] (ii) other proposed changes to the BBLLC operating agreement;[29] or (iii) any other matter of governance or activities within the purpose of the BBLLC."[30]

[24] Specifically, subdivision 4173(2) and subsection 4174(a) of Vermont Business Corporations (11 V.S.A.).

[25] 11 V.S.A. § 4173(1).

[26] 11 V.S.A. § 4173(2)(A).

[27] 11 V.S.A. § 4173(2)(B).

[28] 11 V.S.A. § 4173(2)(C)(i).

[29] 11 V.S.A. § 4173(2)(C)(ii).

[30] 11 V.S.A. § 4173(2)(C)(iii).

Subchapter 12 allows BBLLCs to “adopt protocols to respond to system security breaches or other unauthorized actions that affect the integrity of the blockchain technology utilized by the BBLLC.”[31] In addition, the BBLLC is free to “provide how a person becomes a member of the BBLLC with an interest, which may be denominated in the form of units, shares of capital stock, or other forms of ownership or profit interests.”[32] Finally, the BBLLC is allowed to “specify the rights and obligations of each group of participants within the BBLLC, including which participants shall be entitled to the rights and obligations of members and managers.”[33] What constitutes a member or manager is our next subject.

d. Members and Managers

Under subchapter 12, someone associated with the BBLLC does so as a matter of role. For example, a “member or manager of a BBLLC may interact with the BBLLC in multiple roles, including as a member, manager, developer, node, miner, or other participant in the BBLLC, or as a trader and holder of the currency in its own account and for the account of others, provided such member or manager complies with any applicable fiduciary duties.”[34] Fortunately, these roles may be done remotely, and in fact Vermont assumes that these activities will *not* take place within Vermont. Subchapter 12 specifies that the “activities of a member or manager who interacts with the BBLLC through multiple roles are not deemed to take place in this State solely because the BBLLC is organized in this State.”[35]

e. Consensus Formation Algorithms and the Governance Process

Central to the functioning of a blockchain is its method of *consensus*. This is essential because the distributed nature of the blockchain requires that the various nodes making up the blockchain be identical in both the instructions of the software and the data that is processed with that software. Consequently, with respect to the functioning “in its governance, a BBLLC” may “adopt any reasonable algorithmic means for accomplishing the consensus process for validating records, as well as requirements, processes, and procedures for conducting operations, or making organizational decisions on the blockchain technology used by the BBLLC.”[36] In addition, BBLLCs also have the right to “modify the consensus process, requirements, processes, and procedures, or substitute a new consensus process,

[31] 11 V.S.A. § 4173(2)(D).

[32] 11 V.S.A. § 4173(2)(E).

[33] 11 V.S.A. § 4173(2)(F).

[34] 11 V.S.A. § 4174(a).

[35] 11 V.S.A. § 4174(b).

[36] 11 V.S.A. § 4175(1).

requirements, processes, or procedures that comply with the requirements of law and the governance provisions of the BBLLC."[37]

f. Relation to Other Vermont Laws

The Vermont legislature clipped the scope of the legislation, declining to give it any special preemption over other laws.[38]

IV. Conclusions

Vermont has enacted the first statute that not only allows but actively facilitates the use of blockchains within corporations. While the filing requirements are more stringent, those filing requirements are not onerous. Some of the unanswered questions relate to what happens *after* those documents have been filed. If the BBLLC adopts a significantly differently designed blockchain (or another blockchain altogether), would that fact have to be disclosed to the Secretary of State? Finally, while facilitating the use of blockchains, the Vermont statute stops short of facilitating entirely digital corporations (DAOs) that have no (human) managers or employees.

About the Author

Ronald Chichester is a solo practitioner in Tomball who specializes in technology-related legal issues. He is past chair of both the Business Law Section and the Computer & Technology Section. Ron is a former adjunct professor at the University of Houston where he taught courses in computer crime and e-commerce. He is a registered patent attorney, a certified computer forensics examiner and a certified information systems auditor. Ron received his JD from the University of Houston and he holds a bachelor's and a master's degree (both) in aerospace engineering from the University of Michigan.

[37] 11 V.S.A. § 4175(2).

[38] *See* 11 V.S.A. § 4176.

EDPB Guidance on GDPR's Jurisdictional Scope

By Thomas W. Hayde and Ben Shantz

For many U.S. organizations, the process of figuring out whether (and to what extent) Europe's General Data Protection Regulation (GDPR) applies to their operations has caused a lot of headaches. The process includes answering complicated questions such as

i. Do you have an "establishment in the [European] Union"?
ii. Are you "offering…goods and services…to…data subjects in the Union"?
iii. Are you "monitoring" the behavior of data subjects in the Union?
iv. How will these terms be interpreted and enforced?

The European Data Protection Board (EDPB), which is the working group of EU data protection regulators, recently issued guidelines (subject to revision) in an effort to clarify the territorial scope of the GDPR and to help businesses answer some of the above-listed questions. The followings are some key takeaways from the Guidance concerning the jurisdictional "criteria" under GDPR Article 3:

Even a Minimal "Stable Arrangement" Will Trigger GDPR

GDPR Recital 22 states that "Establishment implies the effective and real exercise of activity through stable arrangements," and that the legal form (*e.g.*, branch, subsidiary, affiliate) is irrelevant to the inquiry. But, what is a sufficiently "stable arrangement"?

The Guidance makes clear that pre-GDPR case law from the Court of Justice of the European Union (CJEU) (in the *Google Spain v. Costeja* and *Weltimmo* cases) will remain good law. The EDPB points out that "[t]he threshold for 'stable arrangement' can actually be quite low." For instance, a U.S-based online retailer having a single employee or agent based in the EU likely would be sufficient to constitute "an establishment in the Union." Any operations—even if minimal—carried out through that single agent will be sufficient to make GDPR applicable to all processing activity related to those operations. Further, again following *Costeja*, any processing "inextricably linked" to the operations of the EU establishment will be covered by the GDPR, no matter where the processing takes place.

What is "inextricably linked" is a case by case, fact-specific analysis, but the Guidance also emphasizes the broad construction to be given to this inquiry.

Outsourcing Data Processing to the EU Will Not trigger GDPR

The Guidance also makes clear that, simply because a U.S.-based data controller chooses to outsource certain processing to a processor based in the EU, it does not mean that controller will become subject to GDPR. The processor is not an "establishment" of the controller in this scenario. However, be mindful that the EU data processor will be subject to the GDPR and will likely seek to impose certain GDPR-related obligations on the controller through a data processing agreement.

GDPR's Extraterritorial Reach Only Applies to "Targeting" of Subjects in the EU

The Guidance confirms that the extraterritorial reach of GDPR is limited. Merely because your website is accessible in the EU does not necessarily mean you are "offering goods and services" or "monitoring" data subjects in the EU. Also, merely because a data subject is present in the EU when you process their data does not mean you have "targeted" EU data subjects with respect to that activity.

The key inquiry is whether you are "targeting" EU data subjects by your activities. Again, following pre-GDPR case law, the Guidance offers several non-exhaustive factors to be considered, including:

- Specifically mentioning or referencing the EU or a Member State in relation to the offering, whether through
    - targeted marketing campaign;
    - use of EU-specific top-level domain names;
    - providing EU-specific contact information (*e.g.*, including applicable international codes);
    - providing EU-specific travel instructions to consumers;
    - use of EU languages;
    - accepting EU currencies; or
    - offering the delivery of goods in the EU; and
- Taking specific actions to facilitate EU data subjects' access to your site.

The Guidance offers two contrasting examples. First, a U.S.-based tech company providing a smartphone application that offers targeted advertising and consumer suggestions based on location information to consumers in markets worldwide including London, Paris and Rome, would trigger GDPR: the company is offering services to data subjects while they are located in the EU. Second, a U.S. news outlet that provides a smartphone app solely to the U.S. market, but that can be accessed by a U.S. citizen while on vacation in the EU (and that collects and processes that subject's data while in the EU), does not trigger GDPR: the company has not "targeted" EU data subjects.

Whether a data subject is "in the Union" is determined at the time the relevant trigger activity takes place, *i.e.*, the moment of offering goods and services, or the moment of monitoring behavior—regardless of the duration of the offer or the monitoring.

Using "Cookies" Does Not Necessarily Trigger GDPR

The EDPB confirms the view that "monitoring" triggers GDPR only where it is purposeful, rather than inadvertent and tangential. Thus, not all use of "cookies" or other passive browser data-collecting technologies will constitute "monitoring." The EDPB emphasizes that what matters is the purpose for which that data is collected and perhaps most importantly what is actually done with it. Processing of such data that allows for what the EDPB labels "behavioral analysis" or "profiling" will be considered "monitoring" to trigger GDPR. The Guidance provides as an example of "monitoring" that will trigger extraterritorial GDPR application: a U.S.-based marketing firm that consults on the layout of a retail store in France based on WiFi tracking of customer movement through the store. Unfortunately, the Guidance does not provide an example of what type of cookies use will not trigger GDPR under the "monitoring" prong. Taking from the marketing consultant example, a cautious organization may fairly extrapolate that using browser analytics that constitute "tracking of natural persons on the internet" and that provide data which are not anonymized will carry a substantial risk of triggering GDPR.

The 3/2018 Guidance on the jurisdictional scope of GDPR is helpful in many respects but leaves many important questions open—especially for organizations with websites accessible to EU-based data subjects and that are using cookies and other browser analytics.

About the Authors

Thomas W. Hayde, CIPP/US. As a privacy professional, Tom Hayde aids clients in developing comprehensive strategies to address information practices and data breach risks, avoid potential claims and liabilities, and ensure compliance with all relevant legal requirements. Tom also helps clients develop and implement protocols surrounding how to respond when a data breach occurs and defends clients against potential claims and lawsuits regarding data breaches. He has experience defending against and resolving civil claims and enforcement actions under specific information privacy laws, such as FCRA, GLBA, HIPAA and RFPA.

Ben Shantz is a civil and commercial litigator who helps developers and contractors by fighting for their interests both in and out of court so they can get back to growing their businesses. In addition to defending businesses inside the courtroom, Ben advises businesses on information privacy and data security needs to protect customers and their information.

Where approved Power of Attorney forms fail you on Digital Assets and problems your clients or you may not anticipate.

By Joseph Jacobson

I. UFADAA, the Revised Version (RUFADAA), and Texas' enactment of its version "TRUFADAA" (TexasRUFADAA).

In 2014, the Uniform Law Commission ("ULC") updated fiduciary law taking into account digital assets by creating and releasing the Uniform Fiduciary Access to Digital Assets Act.[1] This model act was revised and was released as the Fiduciary Access to Digital Assets Act. Revised (2015) ("RUFADAA," the Revised UFADAA).

Some attorneys and scholars may find it unusual or noteworthy that after significant deliberation, the ULC issued the UFADAA, and yet within a year had to revise the act and reissue it as RUFADAA. Be that as it may, in 2017, Texas passed its version of RUFADAA making only slight changes (known as TRUFADAA). That act is codified at Texas Estates Code § 2001.001 *et seq*.

Professor Gerry Beyer[2] was Chair of the Legislative Committee of the Real Estate Probate and Trust Law Section ("REPTL") that reviewed the ULC's version of RUFADAA. His committee offered statutory changes and commentary to make it compatible with Texas laws. This author was one of REPTL's Legislative Committee members working with Professor Beyer.

Texas was among the most recent states to enact the law, which has been adopted by about 40 states and the U.S. Virgin Islands.[3] The law treads in relatively novel legal territory and raises a host of interesting questions, some of which are presented in this article.

[1] Katie Robinson, "Uniform Law Commission: An Update for Legislative Lawyers," May 19, 2015, http://www.ncsl.org/legislators-staff/legislative-staff/research-editorial-legal-and-committee-staff/uniform-law-commission-an-update-for-legislative-lawyers.aspx.

[2] Professor Gerry Beyer, Governor Preston E. Smith Regents Professor, Texas Tech University School of Law. http://www.professorbeyer.com/Beyer/About.html.

[3] Uniform Law Commission, Fiduciary Access to Digital Assets Act, Revised, Legislation, https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22.

II. A Digital Assets Fiduciary’s potential liabilities,

A. May an attorney properly deny a Digital Assets Fiduciary’s request to access a Principal’s digital legal documents including attorney-client privileged communications (emails) between the attorney and the Principal?

A lacuna exists in Texas case law so the full impact of the definition of a digital asset is not settled.[4] A digital asset may include information that is subject to the attorney-client privilege as to the original Principal, *i.e.*, the person granting the fiduciary access to the digital assets.

Often digital assets are not enumerated. They are identified broadly by their characteristic—the asset is digital. Because they are in digital form, the assets may be easily transferred. A person may have digital assets stored on servers at Microsoft’s Azure or in Microsoft’s 365 Office. These same assets may be stored simultaneously or transferred to Amazon Web Services (“AWS”) or some other Cloud Service Provider (“CSP”). Instagram, Facebook, and Whatsapp are also considered digital assets even though many people do not think of these social media sites as Cloud Computing or places where digital assets may be stored.

The statute properly allows for this flexibility appropriate to the identity of the asset. It would be difficult and cumbersome for a Principal to continually update his or her digital power of attorney to include the Principal’s administrative changes. These matters could be communicated outside the TRUFADAA-compliant document.

Even if there are no changes in CSPs, the Principal would also want to update the Fiduciary as to User IDs and Passwords necessary to access the various digital accounts. Under the best practices these User IDs and Passwords would be changed at least annually. User IDs and Passwords may be best transmitted in an encrypted form as between the Principal and the Fiduciary, rather than stated within the TRUFADAA document. The TRUFADAA Power of Attorney may be seen by people with whom the Principal would not want to have access to the digital data.

A “digital asset” does not include the asset or liability that underlies the digital representation. So, for example, a Fiduciary’s controlling a digital deed for real estate does not include the Fiduciary’s control over the real property described in the deed.

[4] “‘Digital asset’ means an electronic record in which an individual has a right or interest. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record.” Tex. Est. Code § 2001.002(8) (2017).

If your attorney drafts a will or a trust and stores a scanned copy of the signed and witnessed original on a digital device, then that document is a digital asset. That asset is an electronic record in which you, as the Grantor or Testator, has a right or interest. You may have communicated with your attorney through emails, and your email account would be a digital asset to which your Fiduciary under TRUFADAA would also have access.

These email communications between your attorney and you could be accessed through your attorney's records, as well as the records that you may have kept in your email account.

The concern that is troubling some attorneys, particularly those with an estate planning practice, is, "What is the appropriate response when a Digital Assets Fiduciary seeks the will or trust documents and all digital correspondence between the Principal and the law firm relating to the will or trust?"

The attorney who performed the estate planning would want to determine at least two issues:

1. Does the TRUFADAA-compliant Power of Attorney reach the digital version of the will or trust and the digital communications that would otherwise be protected between the Principal and his or her attorney through attorney-client privilege?
2. Does granting the Fiduciary access to the attorney-client communications constitute a waiver of the attorney-client privilege by the Principal-Client?
   a) Was the Principal-Client sufficiently informed that the Fiduciary's exercise of access to the otherwise confidential communications would constitute a waiver of the attorney-client privilege?
   b) Was the Fiduciary informed sufficiently that the Fiduciary's exercise of access to the otherwise confidential communications would constitute a waiver of the attorney-client privilege?

Currently, Texas does not have a case that addresses these issues with TRUFADAA.

B. Is a Digital Assets Fiduciary liable for Digital Assets Information in the Principal's file that may or may not be with the Principal's attorney?

Assume Jane grants Bob her Power of Attorney over certain real estate and also appoints Bob as her Digital Assets Fiduciary. Jane is in Paris, France, and asks Bob to sign the Deed for her conveyance of Dangerous Acres to Mr. Une Whitting. Bob says "Sure," shows up and signs the Deed and other documents making reps and warranties about undisclosed liabilities.

Mr. Une Whitting sues Bob and you (Jane's attorney). How could that be? Assume that Jane had an engineering report delivered to her as an attachment to an email in her Xmail Account—which is a digital asset. This engineering report in digital form discusses the huge quantities of PERC (perchloroethylene) that lie under Dangerous Acres.

- Since Bob is Jane's Digital Assets Fiduciary, does Bob have an obligation to review Jane's Xmail account before the Dangerous Acres closing?
- Since Jane emailed the report to you, her attorney, do you have an obligation to warn Bob about signing the deed and making the real estate reps and warranties about no undisclosed liabilities or adverse findings regarding the property?
- If you were to warn Bob about making representations and warranties, is that a violation of Jane's attorney-client privilege?
    - Is Bob considered like Jane and has to be treated as your client, and warned not to sign anything about undisclosed liabilities?
    - Assume you already warned Jane about not making representations about undisclosed liabilities; so, do you have to warn Bob, or is warning Jane sufficient?
    - What if you as Jane's attorney are unaware Bob is going to sign the deed using Jane's grant of her Power of Attorney to Bob?
- Does Bob have the obligation to find you (Jane's attorney) and ask you about digital documents (assets) that may be relevant to the real estate closing?
    - What if Jane did not forward the engineering report on PERC to you?
    - Should you ask Bob to go through Jane's Xmail account and check for facts (the engineering report) that raises potential liabilities? In this way, if Bob finds anything, you (Jane's attorney) can review and offer proper legal advice to both Bob and Jane?
- Do you as Jane's attorney have an obligation to advise Bob to consider having his own counsel review his obligations and liabilities under the Digital Power of Attorney since you cannot represent both Jane and Bob?

These questions are not answered within RUFADAA or TRUFADAA. But, they are important and involve a great deal more planning and discussion by you (Jane's attorney) with both the Principal (Jane) and the Digital Assets Fiduciary (Bob) than anyone might first anticipate.

C. *RUFADAA[5] creates an unusual problem for Digital Asset Fiduciaries who may be required to file FinCEN records.*

A person with signature authority for a foreign financial account must file a “Report of Foreign Bank and Financial Accounts (“FBAR”) through the (Financial Crimes Enforcement Network’s (“FinCEN”) BSA E-Filing System, even if this person does not file a federal tax return.[6] This report identifies individuals who have signatory authority over an account(s) with $10,000 in assets at any time during a year.

A curious issue arises out of TRUFADAA, that would be applicable to individuals in Texas as well as individuals in other states under RUFADAA. Let’s examine this example:

- Assume Ashley has a $7,000 digital asset (a bank account in a foreign country). Ashley designates Sandy as a Fiduciary of her digital assets, including this foreign bank account.
- Assume Michelle has a $6,000 digital asset (a bank account in a foreign country). Michelle designates Sandy as a Fiduciary of her digital assets, including Michelle’s foreign bank account.

As a Digital Asset Fiduciary, Sandy now has control over two foreign asset accounts, and the total value of the two accounts is $13,000.

Since Ashley’s account balance is less than $10,000 Ashley does not have to file an FBAR form; the same is true of Michelle since her account balance is less than $10,000.

Sandy has a different situation. Because Sandy is a Digital Asset Fiduciary, she has authority over two accounts that, combined within the past year, had a value over $10,000. Sandy has an obligation to file a FBAR.

It would be best if Sandy were to accept the responsibility of a Digital Assets Fiduciary with the understanding that she would have to file a FBAR. In that way, Sandy could inform both Ashley and Michelle that their accounts would be disclosed to the federal government.

[5] This issue is applicable to any person resident in a state that passed an act based on RUFADAA.

[6] BSA Electronic Filing Requirements For Report of Foreign Bank and Financial Accounts (FinCEN Form 114), Release Date January 2017 (v1.4), https://www.fincen.gov/sites/default/files/shared/FBAR%20Line%20Item%20Filing%20Instructions.pdf link found at U.S. Treasury, Financial Crimes Enforcement Network, “Purpose of the FBAR,” https://www.fincen.gov/purpose-fbar.

Ashley and Michelle may not be aware that they would have to file a FBAR since at no time were either of their accounts worth over $10,000 in the last year. Their advisors (attorneys as well as accountants) may not have mentioned this possibility to their respective clients.

Since the obligation to file rests on Sandy, then she would suffer the penalties for failure to file. These penalties are significant.

Ashley and Michelle may think of the Digital Assets Fiduciary as being more centered on their Instagram, Facebook, and other social media accounts. When independently designating Sandy as their Digital Assets Fiduciary, a foreign account may ***not*** be the within their perceived scope of a digital asset.

For Sandy, failing to file a FBAR could result in fines of $10,000 per year for each year she failed to file for up to six years, or up to 50% of the value of the account(s). The loss of 50% of the two accounts is possible even though the accounts are not Sandy's because Sandy has signature authority over the accounts. If Ashley and Michelle find their accounts diminished by 50%, then Sandy may find herself blocked on Facebook, and Ashley and Michelle might sue Sandy claiming Sandy breached her fiduciary duty by not filing a FBAR.

Before accepting a position as a Digital Assets Fiduciary, it is best to require a full disclosure of all Digital Assets, and a request that this list be updated periodically. Sandy's attorney may even ask that Ashley and Michelle represent that they do not have any control over a foreign bank account or other digital assets.[7]

D. RUFADAA creates a different, but similarly unusual problem for Digital Asset Fiduciaries who may be required to file IRS Form 8938.

IRS Form 8938 requires reporting foreign financial assets if the total value "in which you have an interest" is more than the threshold. A Digital Fiduciary's control over a Digital Asset, even though the asset is not owned by the Fiduciary would be sufficient to trigger the reporting requirement. For example, for an unmarried taxpayer, the filing threshold is $50,000 in value

[7] Mark Aquilio, *Schoolteacher's failure to file FBAR results in $800,000 penalty*, Journal of Accountancy, December 1, 2018. Available at https://www.journalofaccountancy.com/issues/2018/dec/fbar-penalty-mindy-norman.html.

on the last day of the year or more than $75,000 at any time during the year.[8] Even if the Principal filed a Form 8938, the Fiduciary has his or her own obligation to file that form.

The foreign accounts under control of the Digital Asset Fiduciary are aggregated to determine the threshold amount which requires Fiduciary to file Form 8938. The analysis of who has to file is similar to the calculations regarding filing FinCEN Form 114 in the preceding section "C" for Principals Ashley and Michelle, and Digital Asset Fiduciary Sandy.

As before with the FinCEN filing, Digital Asset Fiduciary Sandy may have an obligation to file, even though her Principals Ashley and Michelle would not have those obligations. Ashley and Michelle would want to know from Sandy (assuming she would know) whether Sandy would have to disclose the accounts that either of them hold, while neither Ashley nor Michelle would have to file Form 8938.

E. IRS analysis and FinCEN determinations of exceptions to the filing should be conducted by a tax attorney; this article is not to be considered legal advice.

This author does not practice tax law. Exceptions and exemptions from filing responsibilities may exist or maybe could be drafted within the Digital Asset Power of Attorney document. This author wants to raise the issues associated with control over digital assets, and direct each attorney to make his or her own determinations as to who has the responsibility to file FinCEN or IRS Forms.

As discussed previously, penalties for failure to file FinCEN forms can be draconian, and failure to file IRS forms are significant. Without appropriate disclosures and investigation by the attorney advising the parties, the Client/Principal or the Fiduciary may have claims against the attorney for damages due to negligent failure to disclose material information. Neither the Client/Principal nor the Fiduciary could make an informed decision if critical information regarding federal government filing obligations and penalties are missing.

III. The importance of delineating the Digital Assets Fiduciary's powers.

The Texas case law does not address the extent of a Digital Assets Fiduciary's powers. But, two cases that deal with assignments of rights shed some insight on the types of issues that the Fiduciary might encounter in relation to his or her powers. The first of these cases arises in an ERISA context, and the second in the context of a Stowers claim assignment.

[8] IRS Instructions for Form 8938 (2018) Statement of Specified Foreign Financial Assets, Department of the Treasury, Internal Revenue Service, November 29, 2018. https://www.irs.gov/forms-pubs/about-form-8938.

A. *Is appointing a Digital Assets Fiduciary similar to assigning a cause of action by a Beneficiary in an ERISA Trust?*

An assignment of a claim for insurance coverage is not so broad as to include an assignment of rights to sue an administrator or trustee for breach of fiduciary duty, or to include the beneficiary/assignee's right to waive attorney-client privilege. So, the "fiduciary exception" to the assertion of attorney-client privilege is inapplicable in these instances. A federal court in Texas ruled on this issue by examining the Federal Rules of Evidence and existing case law.

Advanced Physicians, S.C., ("Advanced") received an assignment from Plan beneficiaries for "their rights as participants in the Plan and their causes of action against the Plan to Advanced."[9] Under authority of this assignment, Advanced sued Cigna for violation of the Employee Retirement Income Security Act of 1974 ("ERISA") to recover beneficiaries' benefits under the Plan (payments). In discovery, Cigna claimed some information was subject to the attorney-client privilege. Plaintiffs sought discovery through a motion to compel.

Cigna argued that the assignment to Advanced to recover payments from the Defendants was not so broad as to include an assignment of the right to waive the Plan beneficiaries' attorney-client privilege against Cigna. The appellate court agreed ruling the assignee Advanced does not become a "beneficiary" of the Plan for all purposes just because it had an assignment to collect *payments* due a beneficiary under the plan.

Advanced tried to assert the "fiduciary exception" to attorney-client privilege assertions by a Trustee or Administrator when sued by a Beneficiary. The Trustee has no independent interest in trust administration; so, any legal advice it receives is on behalf of the beneficiary.[10]

Additionally, the appellate court found the assignment focused on recovery of payments from an insurance company and was not so specific to include a beneficiary's assigning to Advanced breach of fiduciary duties claims against Cigna (the ERISA administrator).

The appellate court used traditional rules of construction requiring assigned rights to be specific. Since Advanced was unable to bring a suit against Cigna for breach of fiduciary duties (that right was not assigned), then Advanced did not have the right to assert the "fiduciary exception" to the attorney-client privilege on behalf of the Plan Beneficiaries. The appellate

[9] *Advanced Physicians, S.C. v. Conn. Gen. Life Ins. Co.* Case No. 3:16-cv-02355-G (BT), 2019 WL 1745966, at *2 (N.D. Tex. 2019) (mem. op.).

[10] *Id*. at *1.

court ruled Advanced was not allowed to access the communications between the Cigna and its attorneys which occurred ***before*** Advanced filed its lawsuit.

B. Does a Defendant's assignment of a Stowers claim against his insurance company include assignment of the right to waive attorney-client privilege?

Cooper was covered by Allstate Insurance.[11] A claim was made against Cooper. Cooper assigned his Stowers and other contractual claims to Joseph. Joseph then brought an action against Allstate. The issue was whether Cooper waived his attorney-client privilege in Joseph's discovery proceedings in the Stowers claims against Allstate.

The assignment read in part as follows:

> "I, the undersigned, David Louis Cooper . . . here assign, grant, and convey, all rights, title and interest in and to any causes of action that I may have against Allstate . . . arising out of or by virtue of, my insurance policy or policies, or claims made by Harold Joseph and Mary Joseph . . . against me, including but not limited to any causes of action I may have pursuant to the Stowers Doctrine, Texas Insurance Code, breach of contract, or any other common law fraud, misrepresentation, or other causes of action."[12]

The trial court found that an assignment or waiver of Cooper's attorney-client privilege was encompassed or implied in his assignment of the Stowers action. Allstate appealed.

The appellate court found the assignment inadequate to constitute a waiver of Cooper's attorney-client privilege. The appellate court noted that there was no language in the assignment specifically referencing the attorney-client privilege. Nor was there any language in the assignment that obligated Cooper to participate in Joseph's claim against Allstate.

The appellate court also stated the attorney-client privilege may be waived in accordance with Tex. R. Evid. 511(b)(1), but the court did not find any previous production of documents by Cooper that waived the privilege, since all those documents were properly redacted.

[11] *In re David Louis Cooper*, No. 09-01-122-CV, court of Appeals of Texas, Beaumont, 47 S.W.3d 206 (Tex. App—Beaumont 2001).

[12] *Id.* at 208.

C. Advanced and Cooper offer some direction for further analysis, but written communications and disclosures by Principals and Fiduciaries will be most helpful for attorneys' drafting for compliance with TRUFADAA, or in other states, RUFADAA.

Advanced distinguishes that an assignee of cause of action arising from an ERISA Plan from a Plan Beneficiary does not stand as the Beneficiary. The Digital Asset Fiduciary through the Power of Attorney does stand exactly as the Principal, unless otherwise limited. The Fiduciary could make any decision and take any action consistent with the Principal's direction in the Power of Attorney.

Cooper emphasizes the importance of being very specific as to what powers are granted or denied when referencing the Digital Assets. The court discussed a failure to reference the attorney-client privilege or its waiver. Without this reference, it was easy for a court to hold the power to waive attorney-client privilege was not granted, and there was no waiver.

You as an attorney are faced with determining whether a power of attorney for digital assets in favor of a Fiduciary requires a special description of the Principal's attorney-client privilege associated with the digital assets. Counsel should try answering the following questions when addressing this issue.

- Is the Principal aware that digital assets could mean access to a will or trust or a foreign asset account or some other legal document which the Principal does not want the Fiduciary to examine?
- Does the Principal want the Fiduciary to have the powers to access the will, the trust, or other digital asset?
- Does the Principal want the Fiduciary to have access to the digital asset, but not to the Principal's digital communications with his or her attorney regarding the digital asset?
- If the digital asset is more than a mere document but has value (such as a foreign bank account), has the Principal made the Fiduciary aware of the responsibilities that are required under the Power of Attorney?
- Is there a discussion in the Power of Attorney about costs for filing FBAR reports or other similar documents?
- Unlike the Assignee in *Advanced* (with respect to Plan Beneficiaries), does the Digital Assets Fiduciary become equivalent to the Principal ***for all purposes***? Does the Principal want the Digital Asset Fiduciary to hold these powers?

- Is a Digital Assets Fiduciary a "client's representative" under Tex. R. Evid. 503?[13]

This last issue regarding the Digital Assets Fiduciary acting as a "client representative" may be addressed in discussion with the Principal. If the Principal wants to limit whether the Fiduciary may seek and receive legal advice ***on behalf of the Principal***, then the Power of Attorney Document may include this limitation. If the Fiduciary believes that legal advice is required to fulfill the duties as the Fiduciary determined, then the Fiduciary may resign.

IV. Conclusion: Successful use of Digital Asset Fiduciaries requires comprehensive legal analysis, a good checklist, and disclosure to all parties, so they may make decisions with informed consent.

Attorneys successfully using TRUFADAA with their clients and their clients' fiduciaries will require more communications with all parties regarding technology. This level of competence should be expected and has been placed into the Disciplinary Rules.[14]

The responsibilities should not be taken lightly by the Principal in granting these powers, nor should the Fiduciary accept a grant of authority and powers as a merely casual accommodation for a friend or acquaintance.

The Principal's attorney's and Principal's disclosures of assets and potential government filing responsibilities would be a minimum in discussions with a Digital Assets Fiduciary, before allowing the Fiduciary to accept the assignment. The attorney may wish to advise the Fiduciary that he or she may want to obtain liability insurance.

About the Author

Joseph Jacobson is an attorney in Dallas, Texas where he practices law as it brushes against technology. He is a former adjunct professor at S.M.U. School of Law and has lectured extensively at Continuing Legal Education courses in Texas and in Illinois. He may be reached at joseph@jacobsonlawyer.com and www.linkedin.com/in/joseph-jacobson-8277a518.

[13] *Id.* at *2 (citing *United States v. Jicarilla Apache Nation*, 564 U.S. 162, 165 (2011). Specific to ERISA claims, the Fifth Circuit recognized this "fiduciary exception" in *Wildbur v. ARCO Chem. Co.*, 974 F.2d 631, 645 (5th Cir. 1992), *reh'g denied* 979 F.2d 1013 (5th Cir. 1992) (per curiam).

[14] "Because of the vital role of lawyers in the legal process, each lawyer should strive to become and remain proficient and competent in the practice of law, including the benefits and risks associated with relevant technology." Tex. Disciplinary R. Prof. Conduct (1989) 1.01, Comment 8. https://www.legalethicstexas.com/Ethics-Resources/Rules/Texas-Disciplinary-Rules-of-Professional-Conduct/I--CLIENT-LAWYER-RELATIONSHIP/1-01-Competent-and-Diligent-Representation.

California Leads the Way in IoT Security Legislation

By Seth Jaffe

California's Security of Connected Devices ("SCD") law,[1] which is scheduled to go into effect on January 1, 2020, will require manufacturers of Internet of Things ("IoT") devices to include reasonable security features appropriate to the nature and function of the device. At the very least, these security features require IoT devices to have either unique preprogrammed passwords or a security feature obligating end-users to set a password before first using the IoT devices. Even though it is not comprehensive in its protections, California's SCD law beats others out of the gate, including several federal laws currently stalled in Congress.

Internet of Things

IoT devices take many shapes but generally refer to any physical object that connects, or is capable of connecting, to the Internet. Obvious examples of IoT devices include a security system that sends video to a homeowner upon an event or a smart watch that notifies the wearer's physician of a health problem. Then, there are the more unusual IoT devices such as Smalt—a smart salt shaker that monitors the sodium intake of its users. And of course, even more extreme examples of IoT devices come out every day, such as Toasteroid, a connected toaster that prints downloadable designs on one's morning breakfast bread. Notably, California's law restricts the definition of a connected device to one that is "assigned an Internet Protocol address or Bluetooth address." This limitation may exempt from the law devices such as RFID tags that operate using alternate forms of near-field communication.

Reasonableness

Tying legality to "reasonable security," as was done in the California law, introduces legal issues. The Federal Trade Commission ("FTC") just faced such a dilemma in front of the Eleventh Circuit in *LabMD v. Federal Trade Commission*.[2] Holding the FTC's order against LabMD unenforceable because it failed to meet a vague standard of reasonableness, the Eleventh Circuit cast into doubt the fate of several laws, regulations, and guidance documents that mandate or recommend reasonable security measures. California's law, in one sense, addresses this issue by deeming as "reasonable" security features that either require a user to update the device password prior to use, or encode within the device itself a unique password.

[1] Cal. Civ. Proc. Code § 1798.91.04.

[2] 894 F.3d 1221 (11th Cir. 2018).

At the low bar, the law makes clear default passwords are unreasonable.[3] But, the high bar remains vague, and in view of the requirement that a connected device contain reasonable security features "appropriate to the nature and function of the device" and "appropriate to the information it may collect, contain, or transmit," legal clarity will likely be a matter for the courts to decide.

Limitations

California's SCD law fails to provide a private right of action, dedicating enforcement only to the state attorney general or a city, county, or district attorney. Anticipating conflict of laws, California's SCD law expressly withdraws applicability related to connected devices subject to security requirements under federal law, regulations, or even federal agency guidance.[4] Likewise, the law does not apply to anyone subject to the Health Insurance Portability and Accountability Act ("HIPAA") with respect to any activity related to HIPAA.

Critics of the law argue that it did not go far enough, citing weak password management as just one of a number of known IoT security vulnerabilities. As is so often the case with new technology, California's new law serves as a starting place until more is learned about the state of the industry and its associated cyber exposures.

Other IoT Bills

Although California was first to pass an IoT law, other authorities have considered the issue, including the U.S. Congress. Several federal bills were introduced in 2017 alone. But, as of the date of this publication, none have yet been enacted. The following list represents the more notable proposals:

- **SMART IoT Act**[5] – directs the Department of Commerce to conduct a study on the state of the Internet-connected devices industry;
- **DIGIT Act**[6] – convenes a working group to provide recommendations to Congress regarding IoT;

[3] For years, devices like network routers shipped with default usernames and passwords of "admin" and "admin," respectively.

[4] The exact wording is "guidance promulgated by a federal agency pursuant to its regulatory enforcement authority." Nonetheless, because guidance documents are not binding, it will interesting to see whether lesser known or antiquated agency guidelines emerge as a basis of challenge to California's IoT law under this exception.

[5] H.R. 6032, 115th Cong. (2017), *available at* https://www.congress.gov/bill/115th-congress/house-bill/6032.

[6] S. 88, 115th Cong. (2017), *available at* https://www.congress.gov/bill/115th-congress/senate-bill/88.

- **Security IoT Act of 2017**[7] – radio frequency equipment must meet certain cybersecurity standards to be established by the FCC;
- **IoT Cybersecurity Improvement Act of 2017**[8] – mandates that government contractors expressly certify their use of IoT devices as employing industry-standard security protocols;
- **IoT Cybersecurity Improvement Act of 2019**[9] – obligates the National Institute of Standards and Technology ("NIST") to develop recommended standards for the security of IoT devices used by the federal government;
- **Cyber Shield Act of 2017**[10] – directs the Secretary of Commerce to establish a program of voluntary certification and labeling of devices that meet industry-leading cybersecurity benchmarks; and
- **IoT Consumer TIPS Act of 2017**[11] – obligates the FTC to work with the NIST to develop educational resources for the cyber protection of IoT devices.

Conclusion

Some estimates have put the number of connected devices at twenty billion by the year 2020.[12] As more IoT devices record, store, and relay personally identifiable information, regulators are right to see IoT protection as a priority. But, in view of tougher data breach notification laws and associated breach litigation costs, manufacturers may want to get a jump on IoT laws by proactively embedding accepted industry security measures into their products.

[7] H.R. 1324, 115th Cong. (2017), *available at* https://www.congress.gov/bill/115th-congress/house-bill/1324.

[8] S. 1691, 115th Cong. (2017), *available at* https://www.congress.gov/bill/115th-congress/senate-bill/1691.

[9] H.R. 1668, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/house-bill/1668/text; S. 734, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/734/text.

[10] S. 2020, 11th Cong. (2017), *available at* https://www.congress.gov/bill/115th-congress/senate-bill/2020.

[11] S. 2234, 115th Cong. (2017), *available at* https://www.congress.gov/bill/115th-congress/senate-bill/2234.

[12] *See*, *i.e.*, "State of the Market: Internet of Things 2017", Verizon Market Report, available at https://www.verizon.com/about/sites/default/files/Verizon-2017-State-of-the-Market-IoT-Report.pdf.

About the Author

Seth Jaffe serves as the General Counsel of LEO Cyber Security (leocybersecurity.com), a cyber operations company offering seasoned trailblazers and creative practitioners to combat today's cyber skills gap. Seth leads LEO's Cyber Incident Response division, providing clients with a unique cyber crisis management program that utilizes executable procedures, concise directives, and an organizational framework modeled after NASA's Mission Control, where Seth worked for nearly fourteen years. Seth also runs the Law Office of Seth E. Jaffe (sethjaffelaw.com), where he represents clients on matters of technology, data protection and privacy, intellectual property, and aerospace.

The Illinois Biometric Information Privacy Act after *Rosenbach*: A Preview of What's to Come?

By William Smith

When the first *Mission Impossible* movie was released in 1996, biometric readers such as retina and thumbprint scanners were more like spy movie fantasies. Today, many smartphone companies encourage users to unlock their device with a thumbprint[1] or facial scan,[2] and anyone can buy a fingerprint scanner from Best Buy for under $80.[3] Many businesses employ biometric identifiers in a wide range of applications including building access control, user authentication, employee timekeeping, smart speakers, and financial transactions.[4] According to one survey of IT professionals in 2018, 62% of organizations used biometric authentication and an additional 24% planned to use it within two years.[5] As these technologies become more widespread, businesses must ensure that they are using these tools in a compliant way. After a recent decision from the Supreme Court of Illinois, employers and others who collect biometric data in Illinois face higher stakes for getting it wrong, as a pending lawsuit against a Texas-based airport services company will illustrate.

That pending case, *Nedialkova v. Total Airport Services*, concerns an employer that required personnel to clock in and out each day using a fingerprint scanner.[6] The former employee-plaintiff and the proposed class allege that their employer violated the Illinois Biometric Information Privacy Act ("BIPA" or the Act) by collecting their fingerprints without: providing publicly available guidelines for the retention and destruction of the data; informing the subjects in writing that the data was being collected; informing the subjects in writing of the specific purpose and term of storage for which the data was being collected; or obtaining a

[1] Samsung https://www.samsung.com/global/galaxy/what-is/fingerprint-scanner/.

[2] Apple https://support.apple.com/en-us/HT208109.

[3] Best Buy https://www.bestbuy.com/site/digitalpersona-u-are-u-4500-finger-print-reader-gray/4918671.p?skuId=4918671.

[4] University of Texas Center for Identity: Current Biometric Adoption and Trends https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf May 2018.; *see also* Norton https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html May 16, 2019.

[5] Spiceworks https://www.spiceworks.com/press/releases/spiceworks-study-reveals-nearly-90-percent-businesses-will-use-biometric-authentication-technology-2020/ March 12, 2018.

[6] Class Action Complaint, *Nedialkova v. Total Airport Services, LLC*, 2019CH02300, Circuit Court of Cook County Illinois County Department, Chancery Division (filed February 21, 2019).

written release from the subjects. Plaintiff and the class seek $1,000-$5,000 in statutory damages for each violation and injunctive relief.

Nedialkova v. Total Airport Services is one example among many class action lawsuits that have been filed since the Supreme Court of Illinois issued its first ruling on BIPA this January. In that case, *Rosenbach v. Six Flags Entertainment Corp.*, the Court held that no additional injury beyond a procedural violation of the requirements of BIPA was needed for a plaintiff to bring a claim for statutory damages or injunctive relief.[7] Illinois and Missouri employment lawyer Susan Bassford Wilson, a partner at Constangy, Brooks, Smith & Prophete, LLP and Co-Chair of the firm's e-Law Practice Group, expects that "this decision is likely to increase the number of class actions filed in an already employee-friendly state."[8] More generally, the broader trend towards protecting data privacy rights and the unique characteristics and risks posed by biometric data suggest that similar regulation will be adopted in other jurisdictions, a process already underway (see below).

The Illinois Biometric Information Privacy Act

BIPA was adopted by the Illinois legislature in 2008. The Illinois legislature found that the use of biometrics by businesses was growing in Chicago and elsewhere, and recognized that this appeared "to promise streamlined financial transactions and security screenings."[9] At the same time, the General Assembly pointed out that biometrics "are biologically unique to the individual; therefore, once compromised, the individual has no recourse."[10] Therefore, it found that regulating the use of biometrics would serve "the public welfare, security, and safety."[11]

BIPA imposes notice, consent, and data governance obligations on "private entities" handling "biometric identifiers" defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" as well as "biometric information" based on such identifiers.[12] (Hereafter this article will use "biometric data" to refer to both biometric identifiers and biometric information). The definition contains a number of exclusions including "information captured from a patient in a health care setting."[13]

[7] No. 123186, 2019 IL 123186 (Ill. 2019).

[8] Author's email interview with Susan Bassford Wilson, May 15, 2019.

[9] 740 Illinois Combined Statutes (ILCS) 14/5.

[10] *Id.*

[11] *Id.*

[12] 740 ILCS 14/10.

[13] *Id.*

Private entities that possess biometric data are required to develop a written and publicly available policy for the retention and destruction of this data. Notably, the biometric data must be destroyed when the initial purpose of collection has been satisfied or within 3 years of "the individual's last interaction with the private entity," whichever occurs first.[14]

No private entity is permitted to collect or otherwise obtain a person's biometric identifier or biometric information unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.[15]

Private entities are prohibited from selling biometric data.[16] Disclosing biometric data is also prohibited, unless the subject has consented. However, this disclosure restriction has exceptions for financial transactions requested by the subject, disclosures required by state, federal, or municipal law, and disclosures pursuant to a warrant or subpoena.[17]

Finally, private entities are required to process biometric data and protect it from disclosure using methods that meet "the reasonable standard of care" in the applicable industry and that are "the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."[18]

The statute provides a private right of action for any person "aggrieved by a violation" of it, with the ability to recover liquidated damages of $1,000 per negligent violation and $5,000 per intentional or reckless violation, plus attorney's fees and costs. Injunctive relief is also available.[19]

[14] 740 ILCS 14/15(a).
[15] 740 ILCS 14/15(b).
[16] 740 ILCS 14/15(c).
[17] 740 ILCS 14/15(d).
[18] 740 ILCS 14/15(e).
[19] 740 ILCS 14/20.

The Act contains exceptions for evidentiary processes in court and situations where application of the Act would conflict with HIPAA, the X-Ray Retention Act, or the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004. In addition, it does not apply to government agencies or contractors working on their behalf, nor to financial institutions subject to Title V of the Gramm-Leach-Bliley Act.[20]

Rosenbach v. Six Flags Entertainment Corp.

In *Rosenbach v. Six Flags Entm't Corp.*, Stacy Rosenbach sued amusement park operator Six Flags and other defendants under the BIPA on behalf of her 14-year-old son and all other similarly situated persons. She alleged that Six Flags had failed to provide and obtain appropriate notice and consent when it collected her son's thumbprint in the course of issuing him with a season pass to the park. The complaint sought damages for Six Flags' violation of BIPA § 15(b) on the grounds that the defendants:

(1) failed to inform class members in writing that their biometric information was being collected,
(2) failed to inform class members in writing of the specific purposes and retention period of the data collection, and
(3) failed to obtain a written release from the class members before collecting the information.[21]

It also sought injunctive relief under the Act and a common-law action for unjust enrichment.

The defendants moved to dismiss on the grounds that, among others, plaintiff had suffered no actual or threatened injury and therefore lacked standing to sue, and that her complaint failed to state a cause of action for violation of the act or unjust enrichment.[22] The trial court denied the defendants' motion except as to the unjust enrichment claim which it dismissed with prejudice. Defendants sought interlocutory review, which was granted. The trial court certified two questions for review: what injury is required for someone to be "aggrieved" for purposes of (a.) liquidated damages and (b.) injunctive relief provisions of BIPA § 20?[23]

The appellate court determined that a defendant's violation of BIPA alone was not sufficient for a plaintiff to pursue relief under the Act. Instead, it held, additional injury or adverse effect

[20] 740 ILCS 14/25.
[21] *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, --- N.E.3d ---, at *2 (Ill., Jan. 25, 2019).
[22] *Id.* at *3.
[23] *Id.*

must be alleged.[24] Rosenbach petitioned the Supreme Court of Illinois for leave to appeal which it granted.

The Supreme Court of Illinois's opinion focuses primarily on the statutory interpretation of BIPA. It notes that before a private entity is permitted to collect a person's biometric identifier or information, the Act requires that the subject:

(1) be informed that the information is being collected;
(2) be informed of the specific purpose and retention period applicable to the information, and
(3) provide a written release.

The sections providing for a private right of action consisting of actual damages or liquidated damages, as well as attorneys fees, costs, and injunctive relief are also highlighted.[25]

From a statutory construction perspective, the opinion contrasts the Illinois Consumer Fraud and Deceptive Business Practices Act, which explicitly requires "actual damages" to sustain an action, with the AIDS Confidentiality Act which does not require actual damages.[26] The opinion cites Illinois cases going back to 1913 that defined an "aggrieved" person in various contexts to include one whose legal rights alone had been violated.[27]

Based on this analysis, the opinion concludes that the Illinois legislature "has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric identification."[28] Accordingly, a person would be "aggrieved" within the meaning of § 20 of the Act "when a private entity fails to comply with one of section 15's requirements."[29] It also references *Patel v. Facebook Inc.*, a California federal case concerning Facebook's tag suggestions program and its use of facial recognition technology.[30] In *Patel,* the Northern District of California rejected Facebook's argument that a plaintiff alleging only procedural violations of BIPA lacked standing. In rejecting the appellate court's characterization of BIPA violations without additional injury as merely technical in nature, the Supreme Court of Illinois quotes the *Patel* court to stress that procedural protections are especially important in today's

[24] *Id.*

[25] *Id.* at *4.

[26] *Id.* at *5.

[27] *Id.* at *6.

[28] *Id.*

[29] *Id.*

[30] *Patel v. Facebook Inc.,* 290 F. Supp. 3d 948 (N.D. Cal. 2018).

world where digital technology enables "the wholesale collection and storage" of people's unique and unchangeable biometric identifiers.[31]

Finding that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act", the Supreme Court of Illinois reversed the appellate court judgment and remanded to the circuit court.[32]

Next Steps after *Rosenbach*

Because *Rosenbach* substantially lowered the bar for bringing a claim under BIPA, it is critical that lawyers whose companies or clients collect biometric data from employees or consumers in Illinois take steps to ensure their compliance with its requirements.

Organizations with operations in Illinois should:

- conduct a data mapping exercise to identify any points where a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry is being collected from employees or others;
- ensure that appropriate written notice is provided and a written release is obtained prior to collecting biometric data from any person;
- create publicly available policies that describe the retention schedule and destruction guidelines for biometric data, and ensure that they contain a backstop where biometrics will be retained no longer than 3 years after the data subject's last interaction with the organization; and
- review their IT systems involved in processing and storing biometric data to ensure that they meet reasonable industry standards and that they are equivalent to the measures used for other categories of sensitive or confidential information.

Constangy's Susan Bassford Wilson also recommends that organizations carefully evaluate any vendors who are collecting biometric data on their behalf: "Companies should take the time to understand the details of each such system and also consult with counsel who has expertise in this area to determine whether a system triggers obligations under BIPA. Further, agreements with such vendors should be reviewed and revised with this statute in mind. And, if a company

[31] *Rosenbach* at 34, citing *Patel* at 954.

[32] *Rosenbach* at 40.

suspects that they are not in compliance with the BIPA, I recommend swift action to evaluate and address that lack of compliance."[33]

Finally, Texas companies that are considering purchasing organizations in Illinois or their assets should add a BIPA compliance section to their standard due diligence questionnaires.

It seems likely that Illinois's BIPA is a case study in what will become a larger phenomenon. In recent months, laws regulating biometric data have been proposed in New York City, Florida, and at the U.S. federal level.[34] Also, barely a month before this issue went to press, San Francisco became the first municipality to ban the use of facial recognition technology by city agencies.[35] As both the Supreme Court of Illinois and the Northern District of California have observed, the unique characteristics of biometric data—and the attendant possible harms from its use—justify special procedural safeguards.

About the Author

William Smith is Assistant General Counsel of Business Talent Group, LLC (BTG), the leading marketplace that connects independent management consultants, subject matter experts, and executives with top companies to solve their biggest business problems. He leads BTG's data privacy compliance, employment law, and commercial agreements activities. In addition, he closely supports BTG's General Counsel on fundraising transactions, governance and investor matters, and risk management. He is a member of the Council of the Computer and Technology Section of the State Bar of Texas.

[33] Author's email interview with Susan Bassford Wilson, May 15, 2019.

[34] Data Privacy Monitor https://www.dataprivacymonitor.com/biometrics/in-bipas-wake-a-wave-of-new-biometric-privacy-proposals/#page=1 April 15, 2019.

[35] BBC https://www.bbc.com/news/technology-48276660 May 15, 2019.

15 Cases and Statutes in 45 Minutes

By Lisa Angelo, Pierre Grosdidier, Shawn Tuma

(This article will be presented at a speakers' panel at the
June 2019 Texas Bar Conference in Austin, Texas.)

This article briefly summarizes 15 recent cases, statutes, and legal developments that every Texas attorney should know about.

1. Business Duty to Protect Sensitive – Personal Information & Notify of Breach

The Texas Identity Theft Enforcement and Protection Act[1] (ITEPA) requires those engaging in business in Texas (including lawyers and law firms) have cybersecurity and data privacy duties to: (1) implement and maintain reasonable procedures to protect electronic sensitive personal information ("SPI") they collect or maintain;[2] (2) follow appropriate data destruction procedures;[3] and, (3) notify any individual whose SPI was or is reasonably believed to have been acquired by an unauthorized person.[4]

As of this writing, the 2019 Texas Legislature has passed (and it is believed the Governor will sign into law) HB 4390. HB 4390 amends the breach notification law with two major changes: (1) instead of "as quickly as possible," notification now must be made "without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred;" and, (2) a person required to notify 250 or more residents of Texas must also notify the attorney general and provide five specific categories of information.

2. Texas Lawyers' Competence in Technology

The Texas Disciplinary Rules of Professional Conduct were amended in early 2019, expanding a lawyer's duty to maintain competence to include understanding the benefits and risks associated with relevant technology.[5] This amendment follows the trend set by the American Bar Association after it issued a similar amendment to the Model Rules in 2018.[6] Since 2017, the ABA has also issued opinions on lawyers' obligations to protect client data and the proper

[1] Tex. Bus. & Comm. Code § 521.001-152.

[2] Tex. Bus. & Comm. Code § 521.052(a).

[3] Tex. Bus. & Comm. Code § 521.052(b).

[4] Tex. Bus. & Comm. Code § 521.053(b).

[5] Tex. Disciplinary Rules Prof'l Conduct R. 1.01, Cmt. 8.

[6] MODEL RULES OF PROF'L CONDUCT R. 1.1, Cmt. 8 (2018).

steps to respond to a data breach.[7] The opinions reiterate how rules of ethics apply in the digital era.

3. Digital Border Searches

Digital border searches of laptops, tablets, and smart phones (both inbound and outbound) are legal. The key issues are (1) the distinction between basic and forensic searches; and (2) the level of suspicion required for each. No level of suspicion is required for basic searches, which means that authorities can rummage through your devices if they want. Circuit Courts are split regarding forensic searches, some requiring some suspicion, others none. The key cases are: *U.S. v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018); *U.S. v. Cotterman*, 709 F.3d 952 (9th Cir. 2013); and *U.S. v. Touset*, 890 F.3d 1227 (11th Cir. 2018). Separately, Custom and Border Protection ("CBP") issued its revised digital search policy in January 2018 (CBP Directive No. 3340-049A, Jan. 4, 2018, available online). The policy recognizes that CBP may perform basic searches without suspicion. Forensic searches require suspicion and supervision. A special procedure applies to privileged information. For additional information, see Pierre Grosdidier's article in the September 2018 *Circuits*.

4. Consequences of Improper Data Destruction

ITEPA requires Texas business to follow appropriate data destruction procedures[8] and they will face consequences when they fail to do so. The Texas Attorney General has pursued claims against businesses for improperly disposing of documents containing SPI. One such case resulted in a $1,240,000 settlement for disposing of 3,000 medical records in a publicly accessible dumpster.[9] Another case in 2015 also resulted in a settlement for disposing of documents containing SPI in a publicly accessible dumpster.[10]

[7] ABA Comm. On Ethics & Prof'l Responsibility, Formal Op. 483 (2018) (Lawyers' Obligations After an Electronic Data Breach or Cyberattack). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf; ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Securing Communication of Protected Client Information"). https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf

[8] Tex. Bus. & Comm. Code § 521.052(b).

[9] *Armstrong Moving & Storage, Inc. v. Am. Cas. Co.*, 2012 WL 12850261, at *1 (W.D. Tex. Dec. 18, 2012).

[10] *State of Texas v. Maria Olveda and Alliance Health Mgt. & Consulting Inc.*, No. 2015C119048, 45th Judicial Dist. Court, Hidalgo County, Texas.

5. Consequences of Inadequate Security

The Federal Trade Commission ("FTC") complained that Uber Technologies, Inc. made misrepresentations about data security and engaged in unfair practices by failing to provide reasonable security to prevent unauthorized access to personal information.[11] In its complaint, the FTC described a few of the practices it considered unreasonable to protect data such as Uber's alleged failures to require multi-factor authentication and encryption. The FTC complained that based on the unreasonable security controls in place, Uber's statements about data security were misrepresentations.

6. Cell Phone Tracking Without Warrant

In *Sims v. State*, the Texas Court of Criminal Appeals ("TCCA") unanimously held that authorities did not violate a suspect's Fourth Amendment privacy rights when they "pinged" his cell phone less than five times over less than three hours without a warrant to locate and arrest him on suspicion of murder.[12] The decision is consistent with *Carpenter v. United States*, where the U.S. Supreme Court recently held that a warrant was required to access seven days of cell-site location information (CSLI).[13] *Carpenter* was a narrow decision that left room for warrantless requests for CSLI under exigent circumstances, such as when authorities "need to pursue a fleeing suspect, [or] protect individuals who are threatened with imminent harm."[14] For additional information, see Pierre Grosdidier's *Feature Article* in the March 2019 Circuits.

7. Lawyers' Duties to Protect Client Data: Even Paper Files in a Stolen Vehicle?

In recent years the discussion of lawyers' duty to protect client data has focused on digital data, however, those same duties apply to protecting client data in traditional paper form. This issue is front and center in one recent case. MoneyGram hired Mark Kovalchuk to collect old debts from numerous individuals. MoneyGram provided its files to Kovalchuk, which included information about the debts owed and the debtors' credit information. According to the allegations in the lawsuit, Kovalchuk then traveled from Minnesota to Arizona with the hard copies of the files and, along the way, "left boxes of documents containing confidential and/or personally identifiable information in Mr. Kovalchuk's 'tricked out Hummer H2' while it was parked overnight at a hotel in Albuquerque, New Mexico—even though defendants chose to protect and to safeguard other items, such as their laptop and liquor, by bringing these items into their hotel room." The "tricked out Hummer H2 was stolen from the Hyatt Place Hotel,

[11] *In re Uber Tech., Inc.*, F.T.C. Docket No. C-4662, Complaint (Oct. 28, 2018).

[12] 569 S.W.3d 634 (Tex. Crim. App. 2019).

[13] 138 S. Ct. 2206, 2217 n.3 (2018).

[14] *Id.* at 2220, 22-23 ("Our decision today is a narrow one.").

Uptown Albuquerque" and, along with it, the MoneyGram client files containing sensitive personal information of the debtors from whom MoneyGram was trying to collect its debts—individuals that MoneyGram would consequently be required to notify of this data breach. MoneyGram is suing Kovalchuk for gross negligence, among other things.[15]

8. Consequences of Inadequate Security Of Third Parties

Shortly after learning its third-party vendor had unnecessary access to data, BLU Products, Inc. issued a statement claiming to have stopped the vendor's unexpected access. However, the FTC believed otherwise and filed a complaint against BLU for misrepresenting that the vendor's access had been restricted.[16] The FTC also complained that BLU engaged in unfair practices by failing to implement appropriate cybersecurity procedures to oversee the security practices of third-party vendors.

9. *Shore v. Johnson & Bell*, 16-CV-04363 (N.D. Ill., Apr. 15, 2016).

A client initiated a class action against a law firm for its inadequate data security measures. The plaintiffs alleged that the law firm was "a data breach waiting to happen." There was no actual harm and the case move to confidential arbitration, but not before the plaintiffs had made their point.

10. Departing Lawyers and Outlook .pst Files

The facts of this hypothetical situation are intended to help lawyers think about the issues that arise in a situation that happens in law firms every single day: A lawyer decides to leave a law firm and, in preparing to do so, copies to a USB thumb drive his Outlook .pst file that contains all of the emails the lawyer has sent and received on behalf of all clients for whom he has worked while at the law firm. The lawyer then takes the USB thumb drive full of the law firm's client data, saves its contents in its entirety to the network of his new employer, and then loses the thumb drive. Who is responsible for the data on the USB drive? Who is responsible for securing the data on the USB drive? Who is responsible for notifying the entities and individuals that their sensitive information has been lost? Who has ethical obligations to keep confidential the data on the USB drive?

[15] *MoneyGram Int'l Inc. v. Kovalchuk Law Offices PA*, 1:18-cv-01036, U.S. District Court for the District of New Mexico (Nov. 18 – actively litigating).

[16] *In re BLU Products, Inc. & Ohev-Zion*, F.T.C. Docket No. C-4657, Complaint (Sept. 6, 2018).

11. Consequences of Inadequate Security of a Sole Proprietorship

A sole proprietor's claims ensuring security of users' account information by using the latest encryption and security techniques were misleading, according to the FTC's complaint.[17] The FTC also complained that the sole proprietor was engaged in unfair practices based on its unreasonable data security.

12. Consumer Data Protection Act

Senator Ron Wyden (D-OR) introduced S.2188, a bill entitled the "Consumer Data Protection Act" (CDPA).[18] The proposed statute is the first federal foray into consumer privacy laws. The CDPA applies to "covered entities," which are defined as entities that have $50 million or more in annual revenue and that have records for a million or more consumers. The Act would, int*er alia*, define "personal information" very broadly, grant the FTC oversight authority in the domain of consumer personal information, and require the FTC to deploy a "Do Not Track" website that would allow consumers to "opt-out" of data sharing. For additional information, see Pierre Grosdidier's *ShortCircuit* in the December 2018 *Circuits*.

13. Contractual Exclusion in Cyber Insurance

When procuring cyber insurance, it is important for companies to know if the insurance will cover claims that are contractual in nature, such as routine indemnity agreements contained in many contracts. Some policies have language excluding contractual liability, such as an exclusion for "actual or alleged liability under a written or oral contract or agreement."

This exclusion was the focus of a recent case between Spec's Family Partners and its insurance carrier. Spec's had previously had a breach of payment card data and, pursuant to its contract with its merchant bank that processed its payment cards, Spec's was required to pay fines to the merchant bank. The merchant bank sued Spec's and Spec's made a claim for defense on its insurance policy. The claim was denied because, among other things, it was based on a contractual obligation by Spec's to pay its merchant bank. The case ultimately made its way to the Fifth Circuit, which found that, because there were claims that were not contractual in nature (negligence), there was a duty to defend that was triggered.[19]

[17] *In re Grago, individually and d/b/a ClixSense.com*, F.T.C. Docket No. C-1723003, Complaint (April. 24, 2019).

[18] S. 2188, 115th Cong. § 2 (2018) ("Discussion Draft").

[19] *Spec's Family Partners, Ltd. V. The Hanover Ins. Co.*, 739 Fed. Appx. 233 (5th Cir. 2018).

14. Cyber Insurance Dispute

According to its complaint, Mondelez International, Inc. was one of many victims of a ransomware attack known as NotPetya.[20] Mondelez submitted an insurance claim to it carrier, Zurich American Insurance, which was subsequently denied based on a policy exclusion. Mondelez filed suit against Zurich, claiming that the insurance claim was improperly denied. Even though this lawsuit is currently pending, the complaint highlights important considerations for insureds hoping to have coverage for similar cyber threats.

15. *LabMD v. FTC*, 894 F.3d 1221 (11th Cir. 2018)

After more than a decade of litigation, the Eleventh Circuit brought the FTC's case against LabMD to an end. The FTC had taken LabMD, a medical testing company, to task for its lax data security measures. The case resulted in a lengthy and controversial decade of litigation that involved a congressional inquiry and a criminal investigation. The ALJ initially dismissed the FTC's case against LabMD but the full commission reversed, ordering the company to overhaul its security measures. By then, LabMD had ceased all operations for years. The Eleventh Circuit held that "the Commission's cease and desist order is nonetheless unenforceable. It does not enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished. Moreover, it effectually charges the district court with managing the overhaul. This is a scheme Congress could not have envisioned. We therefore grant LabMD's petition for review and vacate the Commission's order." For additional information, *see* Jamie Sorley's *Feature Article* in the December 2018 *Circuits*.

About the Authors

Lisa M. Angelo is a cyber liability attorney and Certified Information Privacy Manager. Her law practice is focused on advising clients on data privacy, cyber insurance, technology contracts, and other matters related to cyber and technology law.

[20] Complaint, *Mondelez Int'l. Inc. v. Zurich Am. Ins. Co.*, No. 2018-L-11008, 2018 WL 4941760 (Ill. Cir. Ct., Oct. 10, 2018).

Pierre Grosdidier is Counsel in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. Pierre divides his practice between construction litigation and construction contract drafting. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), and the State Bar of Texas Computer & Technology Section Webmaster and Circuits eJournal Co-Editor for 2018-19.

Shawn Tuma is an attorney internationally recognized in cybersecurity and data privacy law, which he has practiced for 20 years. He is a Partner at Spencer Fane LLP. In 2016, the National Law Journal selected him as a Cybersecurity Law Trailblazer and Texas SuperLawyers selected him for the Top 100 Lawyers in DFW.

Senators Introduce The DETOUR Act to Ban “Dark Patterns” on Internet

By Pierre Grosdidier

Have you ever received unsolicited emails from a web site you visited briefly and struggled to exit? Have you ever grown frustrated because you could not find the “Close my account” option on an online vendor’s website you no longer wished to patronize? Chances are, you fell victim to Internet Dark Patterns. Dark Patterns are ergonomic ruses on web sites and apps intended to trick users into accepting services, making choices, or, worse, surrendering personal data against the users’ intentions.[1] These ruses or tricks can be drawn from advanced behavioral psychological studies and are designed to favor the entity behind the web site. Recently, Senators Mark Warner (D-Va.) and Deb Fischer (R-Neb.) introduced a bi-partisan bill, the Deceptive Experiences To Online Users Reduction (DETOUR) Act, to partially ban these clever but arguably controversial practices.[2]

The Act would apply to “large online operators,” which it defines as any person that “provides an online service” to “more than 100,000,000 authenticated users . . . in any 30 day period” and that is subject to the jurisdiction of the Federal Trade Commission (“FTC”). An “online service” is a service made available to the public over the Internet, such as a search engine, an email service, or a social media site, but not an Internet access service. The Act’s flagship prohibition bars the creation of user interfaces that have “the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data.” Additionally, in a nod to the fact that Dark Patterns are usually the end result of behavioral research by Internet users, the Act bans large online operators from segmenting their consumers “into groups for the purposes of behavioral or psychological experiments or studies, except with the informed consent of each user involved.” Finally, in an attempt to address the addictive nature of some Internet activities, especially among children, the Act prohibits large online operators from creating online interfaces directed to children “under the age of 13, with the purpose or substantial effect of cultivating compulsive usage, including video auto-play functions initiated without the consent of a user.”

[1] For make information on Dark Patterns, *see* https://darkpatterns.org/.

[2] A bill to prohibit the usage of exploitative and deceptive practices by large online operators and to promote consumer welfare in the use of behavioral research by such providers; to the Committee on Commerce, Science, and Transportation, S. 1084, 116th Cong. (as introduced in the Senate, April 9, 2019).

Apparently mindful that behavioral or psychological studies provide the methodology behind Dark Patterns, the bill would create duties for large online operators that engage in research in this area based on their users' activity or data. The operators would be required to disclose to their users and to the public "any experiments or studies" conducted "with the purpose of promoting engagement or product conversion." The disclosures must occur routinely, but not less than every three months, and must be "clear, conspicuous, . . . and [] not deceptively obscured." Moreover, large online operators must launch an Independent Review Board to police this research, with authority to approve, force modifications, or disapprove the experiments. The Board must register with the FTC and disclose how it will operate and whether its board members might be conflicted.

Additionally, the proposed Act authorizes large online operators to form an association registered with the FTC as a professional standards body, subject to the FTC's approval and authority. The association must have the authority to compel its members to comply with the Act and to impose sanctions of increasing severity up to and including expulsion for non-complying members. The association must welcome within its membership any large online operator and must assure a fair representation of its members through its governing bodies. At least one of its director must represent users and be independent of large online operator. The goals of the association would be

> to prevent exploitative and manipulative acts or practices, to promote transparent and fair principles of technology development and design, to promote research in keeping with best practices of study design and informed consent, and to continually evaluate industry practices and issue binding guidance consistent with the objectives of th[e DETOUR] Act.

Finally, the proposed Act grants rule-making and enforcement authority to the FTC. The FTC

> shall determine an act or practice is unfair or deceptive if the act or practice—
> (A) has the purpose, or substantial effect, of subverting or impairing user autonomy, decision-making, or choice to obtain consent or user data; or
> (B) has the purpose, or substantial effect, of cultivating compulsive usage by a child under 13.

The FTC would be further tasked with developing and promulgating regulations for securing users' informed consent and for overseeing review boards and the standards bodies. This first requirement is significant because it represents the first legislative attempt to regulate online consent, which most users currently grant by click-through without ever giving a moment's thought to the corresponding use terms and conditions.

Senators Warner and Fisher introduced the DETOUR Act on April 9, 2019, and it might be years before this bill, or some variation thereof, becomes law. In any event, the bill's reach is relatively limited because it would apply only to large online operators with more than 100,000,000 users. But, it is arguably a step in the right direction to balance the rights of users and large Internet operators.

About the Author

Pierre Grosdidier is Counsel in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. Pierre divides his practice between construction litigation and construction contract drafting. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), and the State Bar of Texas Computer & Technology Section Webmaster and Circuits eJournal Co-Editor for 2018-19.

OP–EDS:-

Arrestee DNA Solves Crimes and Saves Lives

By Jayann Sepich

For almost a hundred years, investigators have used fingerprints to solve crime. Science has evolved and now DNA is the fingerprint of the 21st century. Even though all states take a DNA sample from convicted felons, thirty-one states have laws mandating that DNA be taken prior to conviction. Over half of those—eighteen states—mandate that a DNA sample be taken at the time of arrest for ALL felony crimes. During the debate of expanding DNA laws, the right to privacy is always considered.

As I write this op-ed, the Texas Legislature is considering HB-1399, which would mandate that a DNA sample be taken at the time of arrest for all violent crimes, sexual assaults and burglaries.[1] HB-1399 would, therefore, broaden the net cast by DNA testing. It can be argued that this net is expanded at the expense of privacy. But, is taking a DNA sample an invasion of privacy? The answer to this question is a resounding "no." The FBI's Combined DNA Index System ("CODIS"), which is the national forensic DNA database, was designed specifically to guard and protect privacy. Let's examine how it works.

> 16,18;15,15;11,12;10,10;9,11;13,14;29,31.2;16,19;10,14;14,14;7,9;21,26; 15,16;9,12;11,11;11,12;19,22.2;14,18;11,17;18,20.

What are these numbers above? Are they numbers from a super lottery? Or maybe they are an offshore bank account number?

These numbers hold even more hope, more promise than winning millions of dollars in a lottery. These numbers have the power to stop serial rapists and murderers before they can bring horrific pain and suffering to one more victim, before they can shatter the lives of one more family.

I know intimately the pain that can result from violent crime. My daughter Katie was a twenty-two-year-old graduate student when a man she had never met raped her, sodomized her, brutally beat her, savagely murdered her and then set her on fire. And it is numbers like these above that finally identified the man and sent him to prison for the rest of his life.

[1] Editors' note: per the Texas Legislature Online website, at the time this issue of Circuits went to press, the Texas House and Senate passed HB-1399 and sent it to the Governor on May 29.

This numerical profile is the only personal identification that goes into CODIS, the database that has solved thousands and thousands of crimes in the past twenty years. They comprise only twenty locations, out of over three billion in the human genome. What's more, genetic scientists specifically chose these twenty locations because they are located in places on the DNA strand that contain **no medical diagnostic information or physical characteristics.** Even an expert geneticist could not determine any personal or private information from these numbers.

This string of number is *my DNA profile*, which I willingly and openly publish, and even include on my business cards because it contains no personal information. Can you tell anything about me? Can you tell the color of my hair? My eyes? Can you tell whether or not I am predisposed to diabetes, cancer or Alzheimer's? Is this an invasion of my privacy in any way? Absolutely not. Those who are worried about privacy can take solace that names are *not* included in CODIS DNA profiles. A name can only be matched back to this record after it is matched to crime scene evidence.

Texas was the first state to take a DNA sample prior to conviction. But, the Texas law is very limited and, in truth, has not been fully implemented. Since blazing the trail to use the powerful science of DNA, Texas has fallen significantly behind other states. Eighteen states, including every state that borders Texas, now take DNA upon arrest for *every* felony crime. And, these states are seeing incredible results. New Mexico, with a population of less than two million, has seen arrestee DNA match to over 1,800 crimes. And an arrest for drug possession in Louisiana identified the 1996 murderer of Crystal Jean Baker, a 13-year from Texas City. A total of 31 states take DNA as a result of a felony arrest.

Opponents of arrestee DNA paint a very bleak future when DNA database are expanded to include samples taken from arrestees. They paint a state where every person who is arrested by law enforcement for any reason has their identification recorded. Forever. Even if eventually exonerated of whatever alleged offense gave rise to the arrest in the first place, law enforcement not only retains that identification, but also shares it with all of its neighboring states and even states hundreds or thousands of miles away.

But, in truth, *this has been happening since the early 1920's when fingerprint technology came into being*. Right now, everyone arrested must be fingerprinted. The federal government enables states to access each other's fingerprint records through the Integrated Automated Fingerprint Identification System ("IAFIS"). IAFIS maintains a national fingerprint and criminal history system that helps local, state, and federal investigators solve and prevent crime. Has this vast database of arrestees led to a reduction of individual civil rights? Hardly. Widespread fingerprinting has been used with much success to advance public safety in a responsible and constitutional manner.

In my daughter's case there was not one fingerprint found at the crime scene or on her body. But, there were five sources of her killer's DNA. Without DNA technology and CODIS, her killer would still be free. He was never a suspect until he was identified through CODIS. Moreover, he would have been identified *three years sooner* had it been legal at that time to take DNA upon felony arrest.

Texas, along with every other state, takes DNA once a person is convicted of a felony. So why should we take DNA at the time of arrest?

Here is a real-life story about how the use of arrestee DNA identification could have saved the lives of eleven women and kept an innocent man out of prison. In California, a serial rapist named Chester Turner was convicted and had his DNA identification taken. It matched 12 previous rapes and murders, including those of two pregnant women. If Turner's DNA had been taken at the time of his first felony arrest (one of over twenty arrests during the fifteen years he was free to rape and murder again and again), he would have been identified shortly after he committed the first murder and would have been stopped before he raped and murdered eleven more women.

And had Turner's arrestee DNA been taken, David Jones would not have been wrongfully convicted of two of those murders and spent eleven years in prison. Jones was finally released after Turner was convicted of rape and compelled to give his DNA sample.

What a difference it would have made to eleven women, their families, their friends—to David Jones and his family—if one cheek swab had been taken when Turner was first arrested.

That is the power of these numbers:

> 16,18;15,15;11,12;10,10;9,11;13,14;29,31.2;16,19;10,14;14,14;7,9;21,26;
> 15,16;9,12;11,11;11,12;19,22.2;14,18;11,17;18,20.

I am not afraid of having my DNA profile—these numbers—being printed in the newspaper or even being held in a government database. I am afraid of the pain and suffering that can be caused by violent crime—crime that can be prevented—with just these numbers.

About the Author

Jayann Sepich is the co-founder of DNA Saves, a non-profit organization that advocates for arrestee DNA legislation. Disclaimer: This op-ed reflects the view of its author and not those of the Computer & Technology Section, the State Bar of Texas, and their respective officers.

23 and Me: Where I am in Legal Tech Competence as I Hit my 23rd Year of Practice

By Mark I. Unger

On May 3, 2019, I hit 23 years. It hit me back. I never thought I'd be a lawyer much less practice for this long. My genetic predispositions coupled with my environmental triggers as an 80's slacker, led me to believe I should never have made it this far. As I look back in the mirror, and in time, many things seem different. The wrinkles that forced their way into how I've come to look at things are a bit surreal. What I expected in my youth turned out to be different. The practice of law is different. I am different. Even though none of this would surprise those that have come before me, it's the realization of the (now known as inevitable) change that catches me unbalanced. In this digital age, balance also seems to be a misnomer. Maybe Tim McGraw said it best when he sang *"Maybe now I've conquered all my adolescent fears. And I'll do it better in my next thirty years."*

This is now, and that was then. I didn't know how to use a computer then in College and I couldn't afford one in Law School. I also often quote Dennis Miller, who I believe said "I'm ADD-OCD, which means I'm constantly changing what I obsess over." The practice of law requires obsession, though I feel older and more tired, and obsessions wane over time. After the 2008 crash came the startups, as big-law vendors dried up their R&D departments, which, let's be honest consisted of buying up legal startups, such as they were and shuttering them for the most part to gain market share. Technology helped me compensate for my (perceived) lesser legal acumen (*i.e.*, grades) and leveled the playing field (I think) against possibly better lawyers. As time would have it, the 'net-splosion' put everyone's' information out there and put privacy concerns at an all-time high. In the perfect 2009, *et seq.* years, when legal bucks dried up, efficiency became necessary, as it always does. Disruption from actual legal tech startups made it cool to be a nerd and when those like Legal Zoom started to further enhance the idea that people didn't want to pay unlimited dollars for legal form-filling, adaptation became the new 'cool.'

Cool fostered cooler and a perfect storm started to rise. Big Law providers started buying up the new tech again (sorta) and now think they're the fishizzle again. Why all the history? Because in this iteration of 'new law,' I Believe that if we don't adapt, we die. The tech competence trend, now standing at 36 States, while vague, will become more specific in the same way that law does, with interpretation, either in case law or writings and presentations in

CLE. Even though there has been a marked slowdown of legal tech CLE in Texas, there has not yet been an uptick in the enforcement against those who might ignore technology. Every day I see bank and credit card account numbers fly around the net like flying monkeys in our Wizard of Oz divorces.

In Texas, I believe the dropping of legal tech CLE followed an uptick of business/money, loss of appetite by attorneys to consume tech-only CLE, resistance by some bar officials, and an infusion of the topics only where necessary, dropped in as icing on a core-CLE-cake. Pair this with the fact that you can get CLE almost anywhere, the webinar trend and the 'we do it because we have to' attitude most of the time, and you get a perfect storm of preference over necessity. In other words, comfort prevails.

The thing is there are truisms in this world. We like to be comfortable. When we are comfortable, we don't like to change. We don't like to be forced to do things we're not good at. Because of this, and because there has either not been a huge payoff (remember, legal spending is up) or a hammer (there have not been many Judges, it seems, that have come down on attorneys or parties for not chasing tech or efficiency standards), the only way it will change is from a combination of slow national trends trickling down (think ABA Model rules) along with another crash that results in forced efficiencies. Combined with the alternative billing models that have cropped up amongst millennials (and some wannabes like myself—though I haven't fully embraced them), when the rain stops or slows, those who are efficient in their core business space will be more successful. However, I do believe the writing is on the wall and as in all other businesses, the practice of law almost always now requires the tools of technology. These tools are used not just for acquiring sensitive and personal information, but for legal research, most of the communication with opposing counsel, our own clients, experts, and internal staff. Given this fact and the fact that we are charged with guarding our client's goals, dreams, problems, and attempted solutions, competence must include some semblance of technology as the tools of the trade.

Even though I can now use a computer, this term now includes our iPads and iPhones, etc., I'm worried about a day when I'll be 'dinosauric' because I can't code or automation will overwhelm my sensibilities, or Artificial Intelligence will start to argue with me about everything. After all, "I am I. And I [sometimes] wish I weren't." It's a brave new world out there Mr. Huxley. Let's hope our "infinite capacity for taking things for granted" doesn't overshadow our desires to be our best legal selves.

About the Author

Mark I. Unger, is a family lawyer, mediator and consultant in San Antonio, Texas. He has been practicing family law almost exclusively since 1996. He has been highly involved with technology and the integration of technology and law since approximately 1998. www.unger-law.com.

SHORT CIRCUITS:-

Space: The Final Frontier of Government Regulation

By Ryan Gardner

Fifty years ago, activities in space were conducted almost exclusively by government actors. But, in today's world, the participation of private commercial entities is becoming increasingly common. For many companies, space offers a realm of new and exciting opportunities. Any entity seeking to participate in these activities must educate itself on the extensive regulatory scheme governing space activities or risk facing stiff penalties for violating federal law. Just ask Sara Spangelo, the CEO of Swarm Technologies, Inc., whose company was recently ordered to pay a $900,000 civil penalty for launching unauthorized satellites into space.[1]

Upon discovering this complex web of statutes and regulations, one might wonder why such regulations exist at all. The answer is straightforward: the United States is obligated by international law to regulate its nationals' space activities and may be held liable for any damage caused by unauthorized activities. The source of this liability is a 1967 treaty entitled the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodie*s to which the United States is a signatory.[2] Under the Space Treaty, the United States may be held liable not only for governmental activities in space, but also for its nationals' activities.[3] This liability extends to damage caused both on Earth and "in air space or in outer space, including the Moon and other celestial bodies."[4] The potential for liability is especially high for damages occurring on the surface of the Earth or to an aircraft in flight because in either instance the United States is strictly liable.[5] The United States, therefore, has a significant interest in assuring its citizens do not engage in any unauthorized space activities.

Pursuant to this interest, the Federal Government has charged various federal agencies with regulating space activities, including the Federal Aviation Administration ("FAA") and the

[1] https://docs.fcc.gov/public/attachments/FCC-18-184A1.pdf.

[2] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, T.I.A.S. No. 6347, 18 U.S.T. 2410 (U.S. Treaty Oct. 10, 1967) [hereinafter the "Space Treaty"].

[3] Space Treaty, Articles VI-VII.

[4] *Id.*, Article VII.

[5] Convention on International Liability for Damage Caused by Space Objects, art. II-III T.I.A.S. No. 7762 (U.S. Treaty Oct. 9, 1973).

Federal Communications Commission ("FCC"). The FAA primarily regulates the launch of objects into space and their reentry, and Congress has charged the FCC with regulating communications satellites.[6] Under this regulatory scheme, it is illegal to operate a satellite in space without the appropriate authorization and licenses from the FCC.[7] In the case of Swarm Technologies, the FCC denied its application to deploy four experimental satellites in space, and it was after the denial that Swarm Technologies decided to launch the satellites anyway. It appears Swarm Technology's case was the first time a company has taken such brazen action in defiance of the FCC, and it has proven to be a costly mistake. On the bright side, the case resulted in the FCC releasing a new Enforcement Advisory to remind satellite operators that they must obtain FCC authorization before launching any satellites into space.[8] Any companies seeking to launch satellites into space would do well to heed this Enforcement Advisory or risk facing the same hefty penalty as Swarm Technologies.

About the Author

Ryan Gardner is an Associate in in Haynes and Boone, LLP's Business Litigation practice group in Dallas. His practice focuses on both appellate and trial matters. He holds a J.D. from Pepperdine University School of Law and was admitted to the Texas State Bar in 2016.

[6] 51 U.S.C. § 50901; 47 U.S.C. § 151 *et seq.*

[7] *See* 47 U.S.C. § 301; 47 C.F.R. § 25.102.

[8] https://docs.fcc.gov/public/attachments/DA-18-368A1.pdf.

LinkNYC: What Sounds Like a Great Idea Can Have Some Serious Downsides

By Ronald Chichester

Earlier this decade, New York City received an idea. The idea was to provide free wi-fi to pedestrians at street level within the city limit. Even though the idea was sound, the *implementation* of that idea precipitated a controversy,[1] and this controversy nicely illustrates why planning with “privacy in mind” is so important.

In 2014, the Mayor of New York City announced the culmination of a bidding process, wherein private contractors would provide roughly 1,000 wi-fi kiosks to the five boroughs of the New York City. Each of the kiosks would provide free wi-fi, phone calls, charging stations for mobile devices, and a tablet that could be used to access city services, maps etc. To fund the kiosks, New York City allowed the installation of two 55-inch displays for time-based advertising. The advertising revenue would be utilized to fund the entire cost of the kiosk network, so that users and taxpayers would not have to pay anything for access to the kiosks. So far, so good.

The system was dubbed “LinkNYC.”[2] A private consortium called CityBridge won the contract to administer the kiosk network in 2014. Before long, however, things started going sour. After much of the up-front money was spent and infrastructure put in place, CityBridge dropped a bombshell. The first privacy policy[3] promulgated by CityBridge allowed for the collection and (indefinite) retention of “vast amount[s] of information about users” that “carries a risk of security breaches and unwarranted NYPD surveillance.”[4] Since the sale of citizen data was not needed to fund the kiosks network, CityBridge was poised to coup a windfall off citizens. Incidentally, New York City was caught flat-footed.

[1] *See*, *e.g.*, Ava Kofman, “Are New York’s Free LinkNYC Internet Kiosks Tracking Your Movements?” (The Intercept, September 8, 2018) available at https://theintercept.com/2018/09/08/linknyc-free-wifi-kiosks/.

[2] The current LinkNYC website can be found at: https://www.link.nyc/.

[3] *See*, *e.g.*, “NYCLU: City’s Public Wi-Fi Raises Privacy Concerns” (New York Civil Liberties Union, March 16, 2016), available at: https://www.nyclu.org/en/press-releases/nyclu-citys-public-wi-fi-raises-privacy-concerns.

[4] *Id.*

Fortunately, citizen-oriented organizations *did* suspect the worst and sounded the alarm. A classic New York-style kerfuffle ensued, the result of which bequeathed a second privacy policy[5] that, even though being more benign than its predecessor, still had much to be desired.

The lesson here is that any city government, such as New York City, should have anticipated that privately owned, data-handling companies might take advantage of their position and provided adequate oversight over those companies on any related projects. New York City's lack of oversight resulted in unnecessary delays to the LinkNYC system, and created many upset contractors and citizen-users.

About the Author

Ronald Chichester is a solo practitioner in Tomball who specializes in technology-related legal issues. He is past chair of both the Business Law Section and the Computer & Technology Section. Ron is a former adjunct professor at the University of Houston where he taught courses in computer crime and e-commerce. He is a registered patent attorney, a certified computer forensics examiner and a certified information systems auditor. Ron received his JD from the University of Houston and he holds a bachelor's and a master's degree (both) in aerospace engineering from the University of Michigan.

[5] *See, e.g.,* "LinkNYC Improves Privacy Policy, Yet Problems Remain" (The Electronic Frontier Foundation, October 4, 2017), available at https://www.eff.org/deeplinks/2017/09/linknyc-improves-privacy-policy-yet-problems-remain.

Beware of Puffery in Your Security Representations

By Seth Jaffe

You've heard it before. "We take your security very seriously," or "we employ the latest security techniques to keep your information safe." If you were to read the privacy policies of your vendors, you might encounter similar statements. Phrases such as these might put your customers at ease, but they can also draw the attention of the Federal Trade Commission ("FTC"), as one did earlier this month.

In its latest cybersecurity-focused enforcement case, the FTC set its sights on ClixSense—a company that allows its users to earn money by viewing advertisements, participating in surveys, or performing online tasks.[1]

Defendant ClixSense[2] represented to its customers that it "utitlize[d] the latest security and encryption techniques to ensure the security of" customers' account information. The FTC asserted that ClixSense did not use the latest techniques, offering as evidence the lack of numerous controls such as up-to-date Secure Sockets Layer ("SSL") certificates, use of cryptographic algorithms, and penetration testing. It further alleged that ClixSense did not implement reasonable access controls[3] such as segregation, password management, and changing default passwords. The defendant's processes, as stated by the FTC in its complaint, failed to meet the minimum data security measures as prescribed by security professionals and, therefore, were not the "latest security techniques."

As is so often the case in Section 5 actions, the sting of a subsequent consent order is worse than the fine. And *ClixSense* was no exception. The FTC's proposed consent order applies to the owner of ClixSense in relation to any businesses he owns for the next 20 years, and requires those businesses to (1) refrain from transferring, selling, sharing, collecting, maintaining, or storing personal information unless they establish and implement, and thereafter maintain, a comprehensive information security program; (2) conduct third-party

[1] FTC Decision and Order, *In re James V. Grago, Jr., individually and d/b/a ClixSense.com*, No. 172 3003 (Apr. 24, 2019).

[2] The complaint listed James Grago as the defendant, doing business as ClixSense.

[3] As an aside, the ClixSense complaint gives us insight into how the FTC is enforcing its Section 5 powers in the wake of the Eleventh Circuit's *LabMD* decision. In *LabMD*, the Eleventh Circuit vacated an FTC order as being too vague and failing to enjoin a specific act or practice. *See LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221 (11th Cir. 2018). By citing specific controls, the FTC's ClixSense complaint seemingly addresses the *LabMD* limitation.

data security assessments every two years; (3) not misrepresent any fact material to the assessments above, (4) submit an annual certification; and (5) monitor compliance and maintain recordkeeping.

Companies looking to steer clear of this sort of FTC action may want to review their privacy policy language to ensure it matches up with the actual security practices and policies. In addition, consider choosing privacy notification language carefully to avoid overpromising security techniques that may lead to a FTC action.

About the Author

Seth Jaffe serves as the General Counsel of LEO Cyber Security (leocybersecurity.com), a cyber operations company offering seasoned trailblazers and creative practitioners to combat today's cyber skills gap. Seth leads LEO's Cyber Incident Response division, providing clients with a unique cyber crisis management program that utilizes executable procedures, concise directives, and an organizational framework modeled after NASA's Mission Control, where Seth worked for nearly fourteen years. Seth also runs the Law Office of Seth E. Jaffe (sethjaffelaw.com), where he represents clients on matters of technology, data protection and privacy, intellectual property, and aerospace.

re:SearchTX Gives Users Access to All Civil Lawsuit Filings in all 254 Texas Counties From a Single Portal

By Kristen Knauf

Multiple courts in multiple counties usually means multiple logins to multiple websites in order to obtain the desired information. re:SearchTX (https://research.txcourts.gov/) solves that problem. By using the same login that you use for eFileTexas, you can now quickly and easily search for case information from all 254 counties via a single portal. You are empowered with access anytime to all the information necessary to stay informed, effective, and successful via a web-based platform that is accessible from any desktop or mobile device. re:SearchTX not only includes pleadings, motions, responses, appeals, and court orders, but also information about your opposing counsel (*e.g.*, what types of cases they file or how they structure their arguments) and the parties in your case (*e.g.*, whether they are actively involved in other similar cases).

Even though re:SearchTX is designed for court personnel and legal professionals, it is also available in more limited capacities to the public, such as self-represented litigants, and the media. re:SearchTX has strict rules about the level of access that each type of users can access, and has implemented a myriad of security mechanisms to ensure the same level of security and privacy that case parties enjoy with in-person document requests at respective clerk's offices. Details about the case types and documents that are available to non-attorneys can be found in the Judicial Committee for Information Technology (JCIT) Standards. Currently, re:SearchTX provides information for all civil cases but not criminal cases. All documents that were e-filed since January 1, 2016, can be found in re:SearchTX. But, users who are not attorneys, judges, or clerks, however, are not be able to see documents e-filed before November 1, 2018.

re:SearchTX is a "freemium" tool. All you need is an eFileTexas account in order to use the search function of the tool. For $99.00 a month, re:SearchTX Plus provides an enhanced experience with exportable search results and customizable alerts on cases, parties, judges, and even other attorneys.

About the Author

Kristen Knauf is a Senior Attorney at the American Heart Association. She is a council member of the Computer and Technology Section of the State Bar of Texas (2017–20). She received her JD from Marquette University and holds bachelors degrees in Spanish and Political Science from the University of Wisconsin.

A few of my favorite and most useful regularly used apps invoked on my Android Samsung S7 Edge:

By Al Harrison

Cam Scanner App

Intsig's CamScanner is one of my most useful apps. I invoke CamScanner frequently to capture images, especially textual images such as receipts prerequisite for expense reports and for potential returns of grocery items, appliances, etc. This spares me searching for receipts that seem to go "missing" way too often! Quite frankly, I am a solo practitioner and I do not want to spend time locating receipts for my accountant. The default app scan options produce a righteous rendition comprising optimal flash, resolution, and document orientation settings. Besides being stored in situ on a digital device and being simultaneously forwarded via email—optionally with password protection and date-expiration, CamScanner also saves images to its own online database enabling the user to avail herself of a full-size keyboard with which to rename a file and to download or share a PDF or JPEG file. All document-images are kept in sync with one another regardless of whether located on an iPhone, Android device, or Intsig web-app. Cam Scanner is available as a limited-function free version or with (highly recommended) full-functionality. The pro version is worth the modest cost!

RingCentral App

The RingCentral app delivers comprehensive, reliable cloud communications effectuated in the form of a unified voice over internet protocol ("VOIP") routinely invoked on my Android mobile device comfortably emplaced in my palm—cost-effectively. A mere tap or two initiates versatile and seamless business-level communications, *e.g.*, voice calls, voicemail messaging, text messaging, texting, and even online faxing, which I typically invoke via email. Thus, my Android smartphone is the only requirement to have fully-functional office communications regardless of whether I'm sitting in my downtown Houston office or elsewhere at a client situs, at a Bar meeting in Austin, or virtually any other remote location. Integrated team messaging and both audio and video online meetings and collaboration are also conveniently enabled via the RingCentral app. Requiring relatively few taps to specify a communication, reasonably-priced RingCentral subscription enables connecting with team members and clients while I'm hither and yon. I can conveniently customize settings and notifications, such as office hours, welcoming greetings and ringtones.

NordVPN App

The NordVPN app expeditiously and effectively activates crucial protection from malware incursion when I'm online via WiFi at public venues such as airports, hotels, Texas Bar headquarters, Starbucks cafes, etc.—when I'm away from my safe and secure brick-and-mortar office in downtown Houston. A NordVPN remote server redirects and encrypts my internet traffic and replaces my normal IP address when websites are being accessed. Accordingly, once my email and password are securely retained on the app, NordVPN security is invoked by a mere tap upon the "QUICK CONNECT" option and I'm connected to a VPN server randomly assigned from a plethora of available NordVPN servers throughout the country. Ironically, since my actual physical geographic location is obscured (*e.g.*, it may appear that I'm invoking a server in Los Angeles or South Dakota, etc.) Google or another online vendor may request confirmation that I'm a legitimate user since my geographic location appears to be abnormal or unexpected. NordVPN isolates data being both stored and transmitted online as if logically confined in a heavily-walled tunnel with the contents therein being encrypted throughout. As any VPN user, I benefit from experiencing the Internet without censorship and surveillance; uninterrupted streaming without threat of buffering and bandwidth throttling; securely sharing or downloading documents remotely of the law office private network or from reliable databases functioning as public or subscriber repositories of source materials such as the U.S. Copyright Office, U.S. Patent and Trademark Office, Texas Bar CLE Library, Thomson Reuters WestlawEdge and Practical Law. Furthermore, NordVPN services are devoid of any record of my online usage metrics such as Internet access times, duration of online sessions, servers invoked, IP Addresses used, websites visited and duration thereof, or content downloaded. Accordingly, all data from entry at one end of the virtual tunnel to data exit at the other end thereof is encrypted and, therefore, safe and secure, inherently satisfying ethical duties relevant to safeguarding confidentiality and propriety of client information. The service that accompanies the app is quite affordable.

LawPay App

The LawPay app enables a law firm to be immediately paid for legal services rendered or for retained legal services to-be rendered, by invoking Affinipay's top-notch, cost-effective secure credit-card and eCheck processing service. Either the LawPay virtual credit card terminal may be invoked on-screen or by swiping a credit card on a lightweight portable card-reader (free with LawPay service), which I plug into my Android port. When using the virtual terminal, any credit card information entered manually is protected using encryption and tokenization, and all major credit cards and eChecks are accepted through Affinipay's secure online portal. Law firm Payment Card Industry compliance (“PCI”) is routinely handled with the guidance and assurance of LawPay procedures, at no charge. Client payments are appropriately separated into an operating account (comprising earned fees) or into an IOLTA account (comprising presently unearned fees). Recurring payments may be scheduled, at no extra charge, to have commensurate transactions automatically executed. Besides being fully integrated into most popular law practice management software applications, LawPay also enables attorneys to seamlessly and instantaneously receive client payments virtually anywhere attorneys are located.

About the Author

Al Harrison is a patent attorney, concentrating on oil and gas and software and practicing intellectual property law in Houston, Texas. He is chair of the GPSolo Division’s Resource Center Committee and a senior advisor to the Book Publishing Board. He is chair of the Data Privacy and Security Committee of the Business Law Section and a past chair of the Computer and Technology Section of the State Bar of Texas; serves on the Advertising Review and the Professionalism Committees; and is a board member of the Texas Bar College.

What is an Aggregator? And Why Do Some Attorneys Find Them Essential?

By Ronald Chichester and Lisa Angelo

Synopsis:

RSS Aggregators download part of (or all) of a blog posting as they are posted. Lawyers can add the major blogs for their practice area, nominally to keep abreast of the changes in those practice areas. Over time, the aggregator will accumulate a significant amount of information. Most aggregators enable the attorney to search the contents for a particular topic. This means that aggregators can become a handy search tool for your practice area.

How is this different than, say, a Google search?

First, the search in the aggregator is more directed. It is likely (as it has been for us in the past) that the key case or change in the law that we need for a particular topical search is in one of the blogs that we track. That gives us a (learned) start on our searches because it leverages better what other attorneys have written in that area, and in many cases a better search than we would have obtained from using Google.

1. Introduction

Lawyers have been overlooking an important research tool—blog aggregators. Often, when an unfamiliar topic land on our desks, lawyers turn to Google and secondary sources for guidance. Many of today's secondary sources include blogs (or Blawgs). Vast amounts of information are available in blogs that were written by lawyers, industry experts, and businesses. Some of the content is just as useful as a crash course on a particular topic. But, with so many blogs available, how do you filter relevant content? How do you search blogs efficiently, while continuing to refer back for content updates?

If you have subscribed to numerous blogs, websites, and newsletters in an effort to track topics of interest, you may have noticed that your email inbox has become chaotic. Worse yet, you rarely have time to sort and read the information provided in each of your subscriptions. Welcome to information overload.

Rather than succumb to the overload of information or otherwise waste precious time searching the Internet, visiting each individual blog for an update, there is a convenient tool to aggregate the information and save you time. These tools are known as blog or RSS "aggregators."

2. What is a Blog Aggregator?

An aggregator is a software application that aggregates information specifically from blogs. Aggregator applications have several different names, such as news aggregator, feed reader, news reader, RSS reader, or (in our case) blog aggregator. The various names are essentially synonymous. All of the aggregators utilize a technology called Real Simple Syndication ("RSS"). As the name implies, RSS syndicates content from websites (particularly blogs) such that the aggregator can obtain part or all of the syndicated content in an automated manner. For attorneys, blog aggregators are particularly useful for those with a niche specialty, or (more often) for general practice attorneys who have to handle widely disparate types of cases, with each case requiring some amount of legal research because they handle that topic so infrequently.

Blog aggregators are widely available for all the major operating systems (Windows, Mac and Linux). Section 4 of this article covers the various aggregator applications. Some are open source (and thus free as in beer), some are licensed for a fee, and some are cloud-based (and may be advertisement ware).

3. Desired Features in a Blog Aggregator

The three must-have features for blog aggregators are:

- Provide great **search** features;
- Provide the ability to **filter content**; and
- Provide the ability to **import/export lists** of blog feeds.

Search capability is, after all, the main reason for using a blog aggregator. Attorneys can set up aggregators to retrieve content based on specific keywords, authors, publications, etc. Some aggregators will also permit you to retrieve content based on *exclusive* keywords, as opposed to inclusive keywords. Note that because you want to search for content with the aggregator, you need to be able to *store* that information on your PC. Some aggregators are pre-configured to destroy old blog postings after a period of time (say, six months). You'll have to check your settings to enable longer time periods if you plan to refer back to a particular post in the future.

Content filtering is particularly useful if you want to glance at content during the day, but don't want to waste a lot of time. Usually the aggregator will allow for some type of filtering, such as showing only the unread postings. Filtering is one area where the various aggregators differ significantly.

Finally, you want to be able to make use of your aggregator quickly and easily, so automatic uploading of the blogs is a must. Some aggregators make this easier than others by providing **import/export** capabilities. Fortunately, there is a common method of loading syndicated content from multiple websites or blogs (multiple RSS feeds) into blog aggregators all at once. So long as the imported file is in Online Processor Markup Language ("OPML") format, the aggregator should be able to read it. Simply download the OPML file, and import it into your blog aggregator of choice. If your aggregator doesn't support importing (and exporting) OPML files, then you shouldn't be using that aggregator; find one with the import/export capability that adheres to common standards. An aggregator that cannot import/export OPML files is the legal equivalent of not being able to understand the Blue Book.

4. Common/Effective Aggregators for Windows, Mac, Linux, and the Cloud

a. The Cloud

There are several online aggregators. The advantage is that you don't have to install any software on your (various) devices, and what you've viewed is the same on each device. The downside is that you must be online in order to see the content, and in many cases, you can't store the content (and thus search for it) for extended periods of time—thus mitigating their utility for attorneys who want to refer back to the information. Of course, access to stored content may not be an issue if you are only using blogs to keep up with trends in particular topics or become familiar with a new topic.

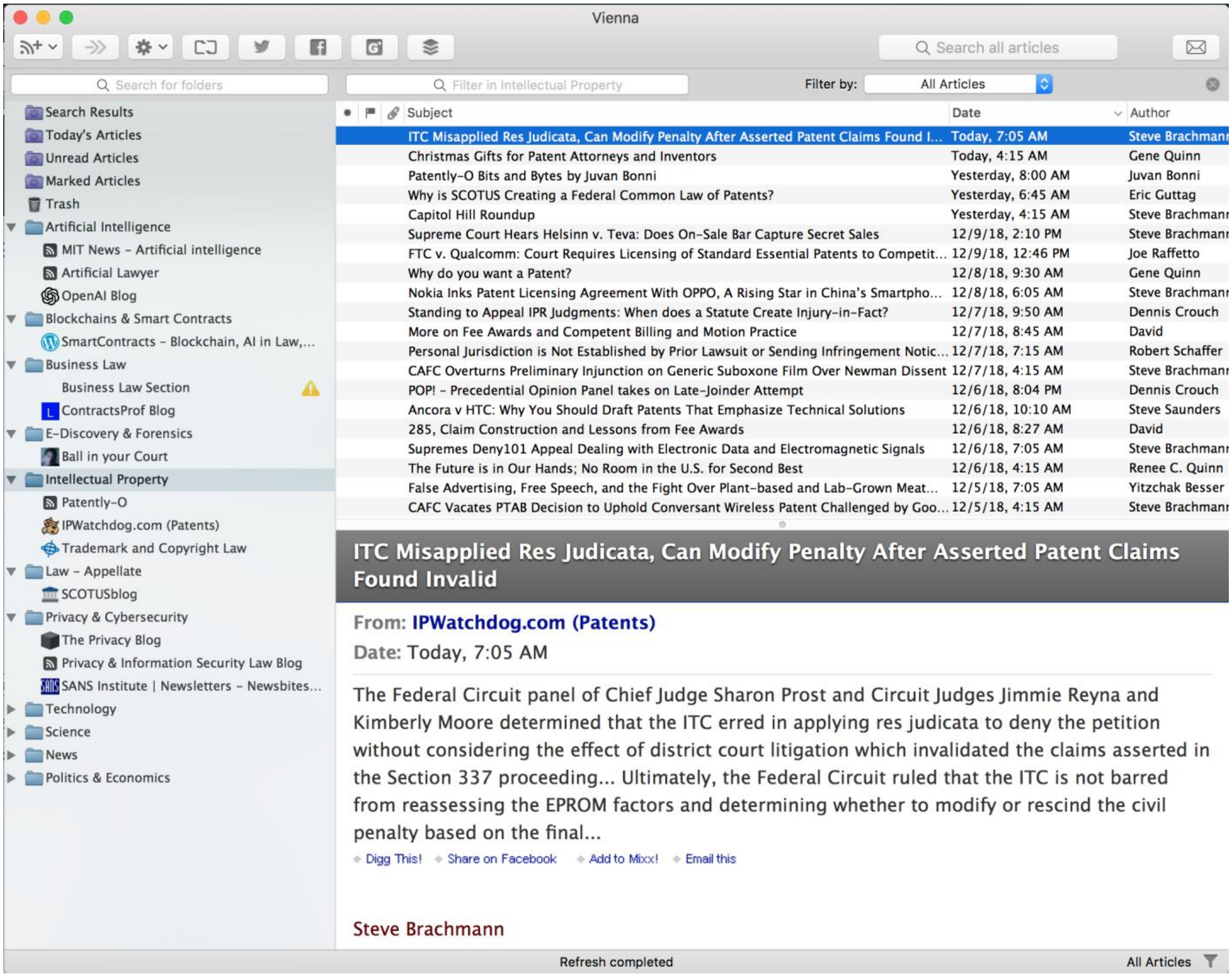
b. Windows

Windows users have several choices. One is called RSSowl. The good news is that RSSowl is cross-platform, which is useful for those attorneys who switch between Windows, Mac, and Linux. RSSowl also has a nifty search feature in that search criteria can be saved and run again later—essentially like its own RSS feed. In other words, you set up a search for a particular legal topic, and then save it. The saved search will show up as a feed and anytime the criteria is met, the particular posting will appear with the saved search. It is this type of filtering that makes aggregators particularly useful for attorneys.

c. Mac

Mac users have fewer choices, but one of them is a real gem: Vienna (see Figure 1). Vienna is quite probably the best blog aggregator on any platform. Vienna is provided under an open source license and is under active development. It has all of the features that an attorney could want (*e.g.*, easy-to-add-blog-feed and a decent search tool). Best yet, it is free to download and use. You can read more about it at their website (http://www.vienna-rss.com/).

Figure 1. Example of an Aggregator: Vienna on Mac OS.



Subject	Date	Author
ITC Misapplied Res Judicata, Can Modify Penalty After Asserted Patent Claims Found I...	Today, 7:05 AM	Steve Brachmann
Christmas Gifts for Patent Attorneys and Inventors	Today, 4:15 AM	Gene Quinn
Patently-O Bits and Bytes by Juvan Bonni	Yesterday, 8:00 AM	Juvan Bonni
Why is SCOTUS Creating a Federal Common Law of Patents?	Yesterday, 6:45 AM	Eric Guttag
Capitol Hill Roundup	Yesterday, 4:15 AM	Steve Brachmann
Supreme Court Hears Helsinn v. Teva: Does On-Sale Bar Capture Secret Sales	12/9/18, 2:10 PM	Steve Brachmann
FTC v. Qualcomm: Court Requires Licensing of Standard Essential Patents to Competit...	12/9/18, 12:46 PM	Joe Raffetto
Why do you want a Patent?	12/8/18, 9:30 AM	Gene Quinn
Nokia Inks Patent Licensing Agreement With OPPO, A Rising Star in China's Smartpho...	12/8/18, 6:05 AM	Steve Brachmann
Standing to Appeal IPR Judgments: When does a Statute Create Injury-in-Fact?	12/7/18, 9:50 AM	Dennis Crouch
More on Fee Awards and Competent Billing and Motion Practice	12/7/18, 8:45 AM	David
Personal Jurisdiction is Not Established by Prior Lawsuit or Sending Infringement Notic...	12/7/18, 7:15 AM	Robert Schaffer
CAFC Overturns Preliminary Injunction on Generic Suboxone Film Over Newman Dissent	12/7/18, 4:15 AM	Steve Brachmann
POP! – Precedential Opinion Panel takes on Late-Joinder Attempt	12/6/18, 8:04 PM	Dennis Crouch
Ancora v HTC: Why You Should Draft Patents That Emphasize Technical Solutions	12/6/18, 10:10 AM	Steve Saunders
285, Claim Construction and Lessons from Fee Awards	12/6/18, 8:27 AM	David
Supremes Deny101 Appeal Dealing with Electronic Data and Electromagnetic Signals	12/6/18, 7:05 AM	Steve Brachmann
The Future is in Our Hands; No Room in the U.S. for Second Best	12/6/18, 4:15 AM	Renee C. Quinn
False Advertising, Free Speech, and the Fight Over Plant-based and Lab-Grown Meat...	12/5/18, 7:05 AM	Yitzchak Besser
CAFC Vacates PTAB Decision to Uphold Conversant Wireless Patent Challenged by Goo...	12/5/18, 4:15 AM	Steve Brachmann

ITC Misapplied Res Judicata, Can Modify Penalty After Asserted Patent Claims Found Invalid

From: IPWatchdog.com (Patents)

Date: Today, 7:05 AM

The Federal Circuit panel of Chief Judge Sharon Prost and Circuit Judges Jimmie Reyna and Kimberly Moore determined that the ITC erred in applying res judicata to deny the petition without considering the effect of district court litigation which invalidated the claims asserted in the Section 337 proceeding... Ultimately, the Federal Circuit ruled that the ITC is not barred from reassessing the EPROM factors and determining whether to modify or rescind the civil penalty based on the final...

Steve Brachmann

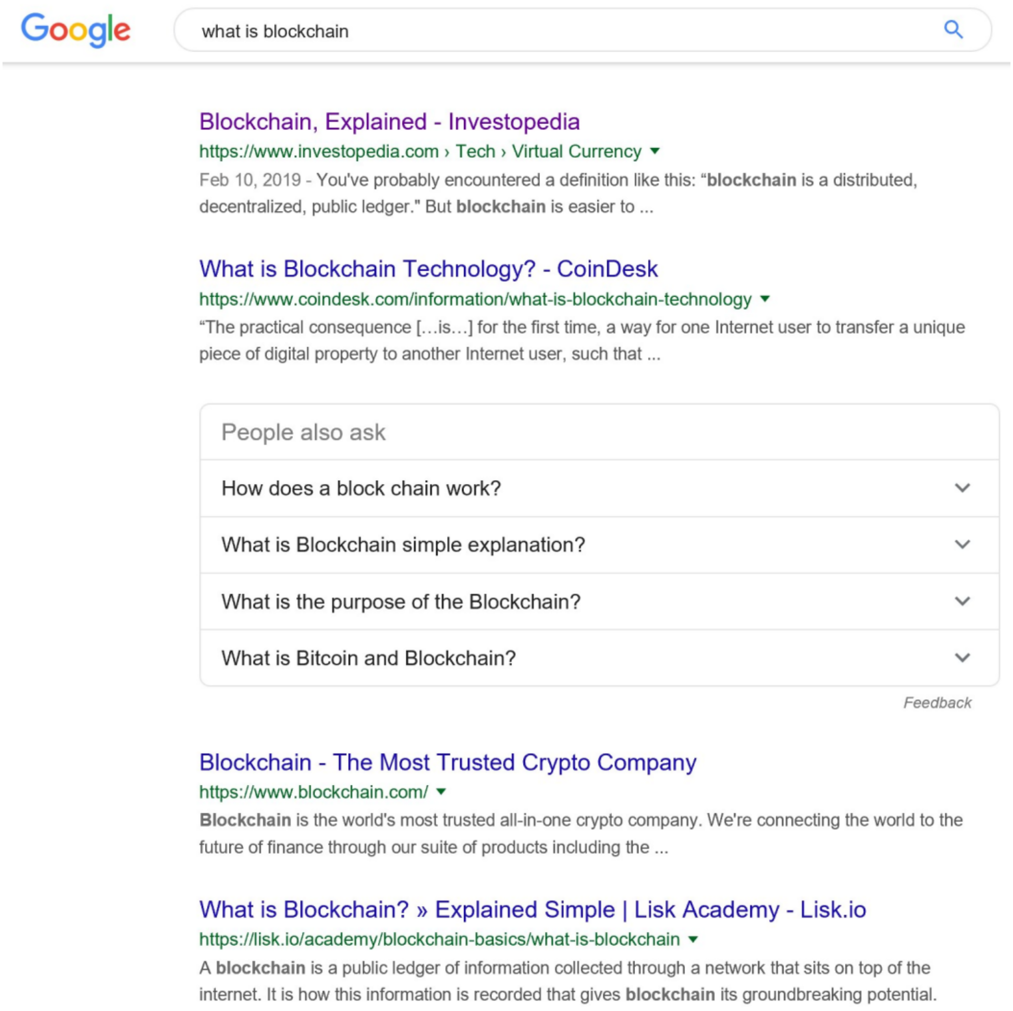
d. Linux

For Linux users, you have several (very good) options. Look here for reviews of the top fourteen (yes, there are 14 popular ones). My favorite is FeedReader. Note, while Akregator is popular in the Linux community, it doesn't let you search for words inside the feeds, so it really isn't much use for attorneys. FeedReader is a great option if you already have some feeds setup online, but is more cumbersome to load new feeds from scratch. FeedReader will, fortunately, allow you to import feeds from OPML files (see above). Once set up, however, FeedReader works quite well. Installation on Linux for these various readers is easy—simply ask for it from your package manager and it will be installed within seconds. Since installation on Linux is so easy, you might want to install several and see which one you like the best.

5. Example Use of Aggregator

Your hypothetical client is interested in using blockchain technology in commercial transactions and wants to know if there are any legal requirements. You know nothing about blockchain and start your research by typing in “blockchain” to your favorite search engine, yielding a variety of results including news articles and blog posts (see Figure 2).

Figure 2 – Google search on blockchains.



what is blockchain

Blockchain, Explained - Investopedia
https://www.investopedia.com › Tech › Virtual Currency ▾
Feb 10, 2019 - You've probably encountered a definition like this: “**blockchain** is a distributed, decentralized, public ledger." But **blockchain** is easier to ...

What is Blockchain Technology? - CoinDesk
https://www.coindesk.com/information/what-is-blockchain-technology ▾
“The practical consequence […is…] for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that ...

People also ask

How does a block chain work?

What is Blockchain simple explanation?

What is the purpose of the Blockchain?

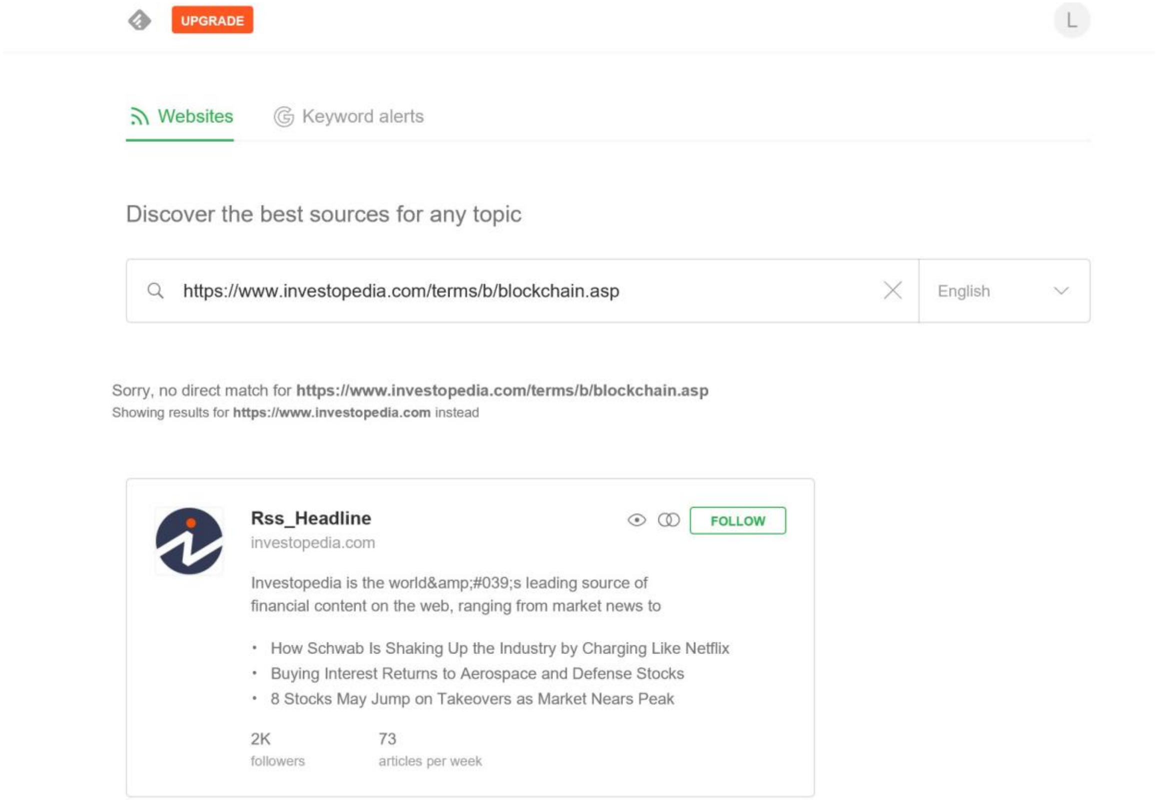
What is Bitcoin and Blockchain?

Blockchain - The Most Trusted Crypto Company
https://www.blockchain.com/ ▾
Blockchain is the world's most trusted all-in-one crypto company. We're connecting the world to the future of finance through our suite of products including the ...

What is Blockchain? » Explained Simple | Lisk Academy - Lisk.io
https://lisk.io/academy/blockchain-basics/what-is-blockchain ▾
A **blockchain** is a public ledger of information collected through a network that sits on top of the internet. It is how this information is recorded that gives **blockchain** its groundbreaking potential.

You find a few sources for which you would like to consolidate the information, search with key words, and use to stay up to date on blockchain. You copy the hyperlink to the sources and add them to your RSS aggregator, in this case Feedly.

Figure 3 – Inserting an RSS feed in Feedly.



Discover the best sources for any topic

https://www.investopedia.com/terms/b/blockchain.asp

English

Sorry, no direct match for **https://www.investopedia.com/terms/b/blockchain.asp**
Showing results for **https://www.investopedia.com** instead

Rss_Headline
investopedia.com

Investopedia is the world&#039;s leading source of financial content on the web, ranging from market news to

- How Schwab Is Shaking Up the Industry by Charging Like Netflix
- Buying Interest Returns to Aerospace and Defense Stocks
- 8 Stocks May Jump on Takeovers as Market Nears Peak

2K followers

73 articles per week

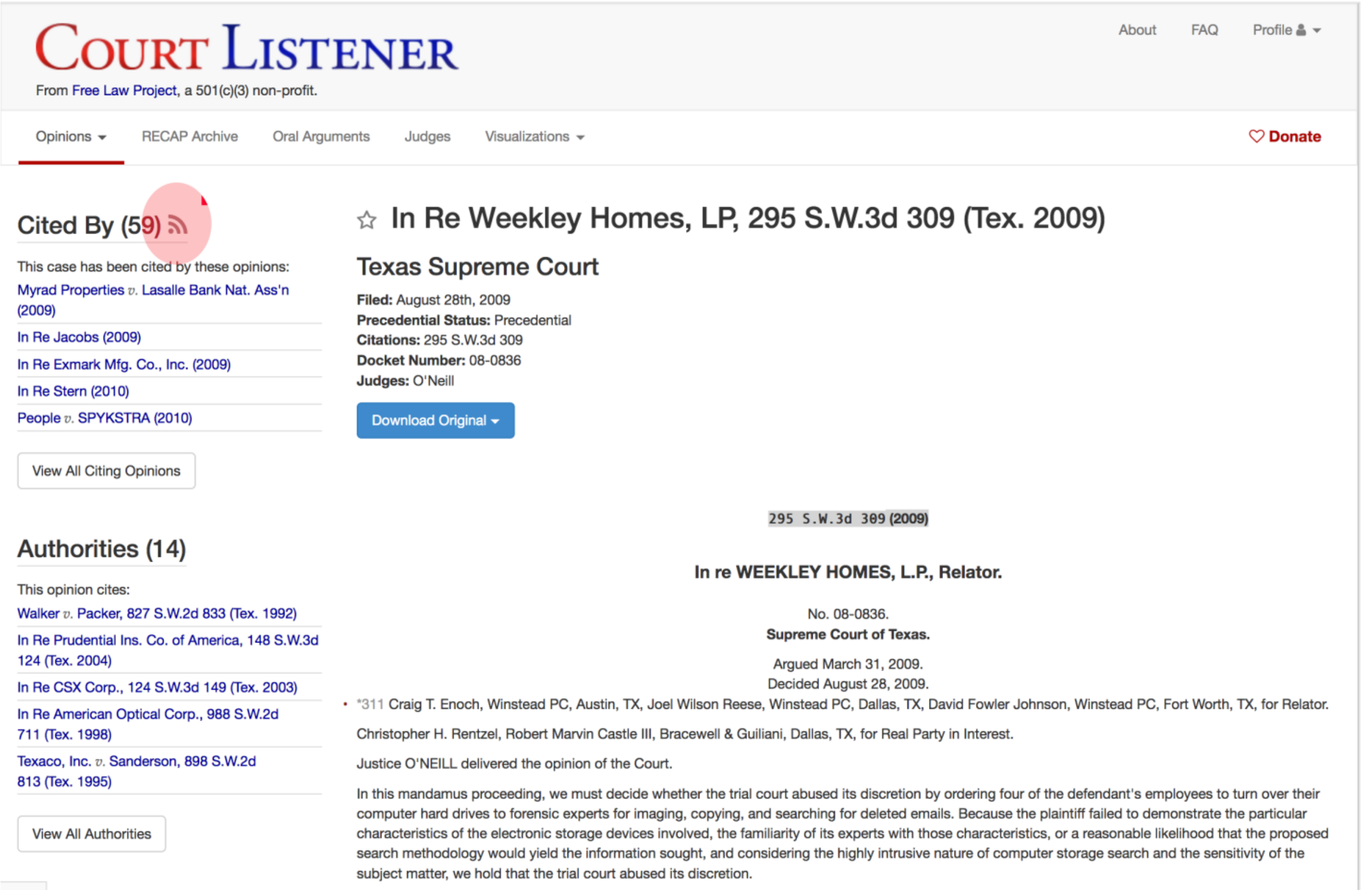
You click "Follow" and repeat for the other resources you found in the initial search.

Alternate scenarios make use of CourtListenter[1] to track key cases in specific areas of the law. For example, if you wanted to track e-discovery cases that cite the seminal Texas Supreme Court opinion *In re Weekly Homes*[2] CourtListener provides an RSS feed for each court opinion that is located next to the "Cited By" in the top-left corner of the web page of the opinion (see below).

[1] *See* https://www.courtlistener.com/.

[2] *In re Weekly Homes, L.P*, 295 S.W.3d 309 (Tex. 2009). Copy available at: https://www.courtlistener.com/opinion/895162/in-re-weekley-homes-lp/?q=texas+supreme+court+in+re+weekly+homes&type=o&order_by=score+desc&stat_Precedential=on&court=tex+texapp+texag.

Figure 4 – Example case from CourtListener.com (with RSS feed highlighted).



Cited By (59)

This case has been cited by these opinions:

- Myrad Properties *v.* Lasalle Bank Nat. Ass'n (2009)
- In Re Jacobs (2009)
- In Re Exmark Mfg. Co., Inc. (2009)
- In Re Stern (2010)
- People *v.* SPYKSTRA (2010)

Authorities (14)

This opinion cites:

- Walker *v.* Packer, 827 S.W.2d 833 (Tex. 1992)
- In Re Prudential Ins. Co. of America, 148 S.W.3d 124 (Tex. 2004)
- In Re CSX Corp., 124 S.W.3d 149 (Tex. 2003)
- In Re American Optical Corp., 988 S.W.2d 711 (Tex. 1998)
- Texaco, Inc. *v.* Sanderson, 898 S.W.2d 813 (Tex. 1995)

☆ In Re Weekley Homes, LP, 295 S.W.3d 309 (Tex. 2009)

Texas Supreme Court

Filed: August 28th, 2009
Precedential Status: Precedential
Citations: 295 S.W.3d 309
Docket Number: 08-0836
Judges: O'Neill

295 S.W.3d 309 (2009)

In re WEEKLEY HOMES, L.P., Relator.

No. 08-0836.
Supreme Court of Texas.

Argued March 31, 2009.
Decided August 28, 2009.

*311 Craig T. Enoch, Winstead PC, Austin, TX, Joel Wilson Reese, Winstead PC, Dallas, TX, David Fowler Johnson, Winstead PC, Fort Worth, TX, for Relator.

Christopher H. Rentzel, Robert Marvin Castle III, Bracewell & Guiliani, Dallas, TX, for Real Party in Interest.

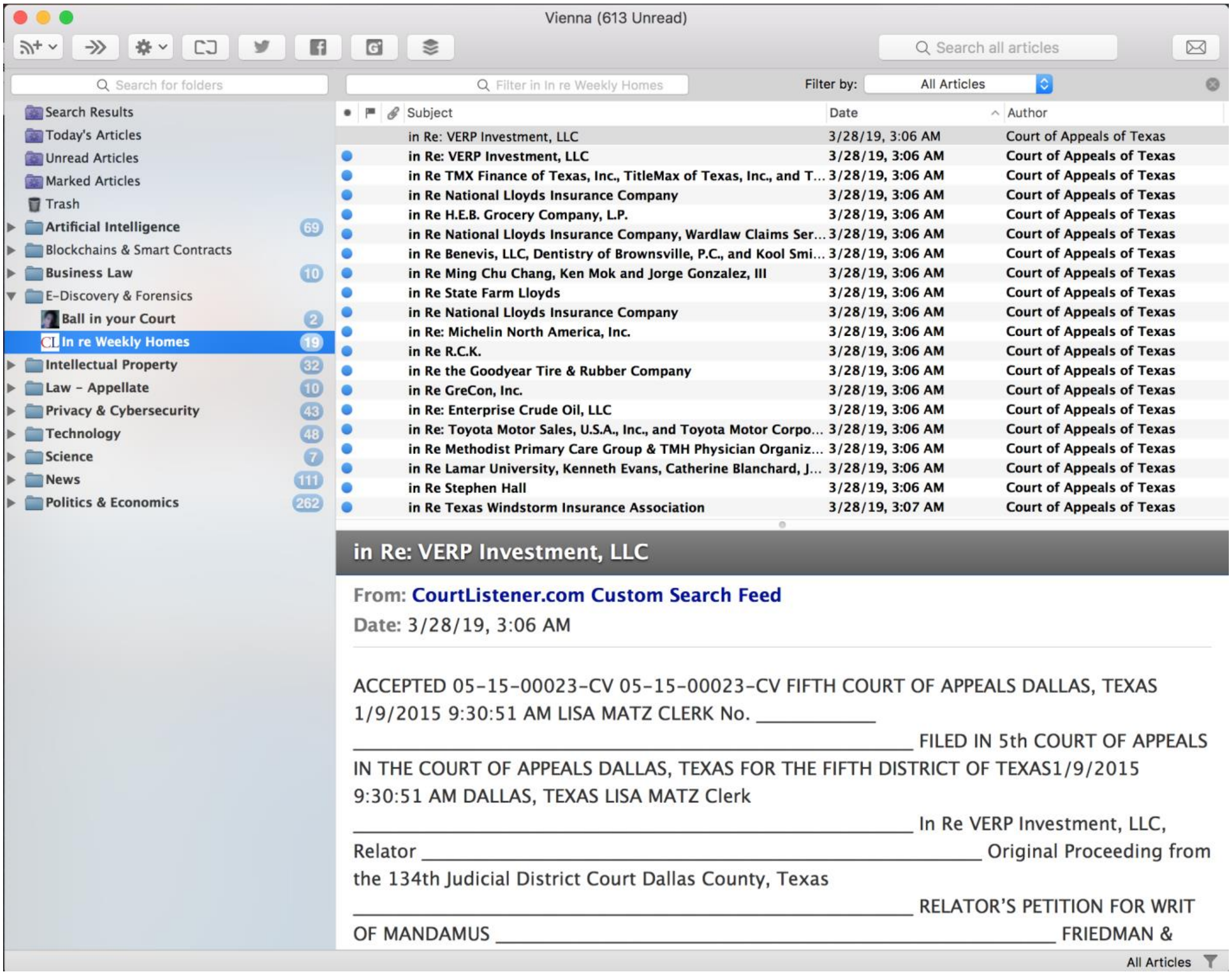
Justice O'NEILL delivered the opinion of the Court.

In this mandamus proceeding, we must decide whether the trial court abused its discretion by ordering four of the defendant's employees to turn over their computer hard drives to forensic experts for imaging, copying, and searching for deleted emails. Because the plaintiff failed to demonstrate the particular characteristics of the electronic storage devices involved, the familiarity of its experts with those characteristics, or a reasonable likelihood that the proposed search methodology would yield the information sought, and considering the highly intrusive nature of computer storage search and the sensitivity of the subject matter, we hold that the trial court abused its discretion.

For the case above, there were (at the time of this writing) 59 cases that cited *In re Weekly Homes*, all of which can be tracked in your aggregator at the designated feed.[3] After that, you can easily track recent Texas e-discovery opinions in your aggregator, as shown below.

[3] https://www.courtlistener.com/feed/search/?type=o&q=cites%3A(895162)

Figure 5 – Vienna with the Texas Supreme Court opinion progeny as a feed.



Filter by: All Articles

●	Subject	Date	Author
	in Re: VERP Investment, LLC	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re: VERP Investment, LLC	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re TMX Finance of Texas, Inc., TitleMax of Texas, Inc., and T...	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re National Lloyds Insurance Company	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re H.E.B. Grocery Company, L.P.	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re National Lloyds Insurance Company, Wardlaw Claims Ser...	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re Benevis, LLC, Dentistry of Brownsville, P.C., and Kool Smi...	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re Ming Chu Chang, Ken Mok and Jorge Gonzalez, III	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re State Farm Lloyds	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re National Lloyds Insurance Company	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re: Michelin North America, Inc.	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re R.C.K.	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re the Goodyear Tire & Rubber Company	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re GreCon, Inc.	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re: Enterprise Crude Oil, LLC	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re: Toyota Motor Sales, U.S.A., Inc., and Toyota Motor Corpo...	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re Methodist Primary Care Group & TMH Physician Organiz...	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re Lamar University, Kenneth Evans, Catherine Blanchard, J...	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re Stephen Hall	3/28/19, 3:06 AM	Court of Appeals of Texas
●	in Re Texas Windstorm Insurance Association	3/28/19, 3:07 AM	Court of Appeals of Texas

in Re: VERP Investment, LLC

From: CourtListener.com Custom Search Feed
Date: 3/28/19, 3:06 AM

ACCEPTED 05-15-00023-CV 05-15-00023-CV FIFTH COURT OF APPEALS DALLAS, TEXAS 1/9/2015 9:30:51 AM LISA MATZ CLERK No. ____________ ____ FILED IN 5th COURT OF APPEALS IN THE COURT OF APPEALS DALLAS, TEXAS FOR THE FIFTH DISTRICT OF TEXAS1/9/2015 9:30:51 AM DALLAS, TEXAS LISA MATZ Clerk ____ In Re VERP Investment, LLC, Relator ____ Original Proceeding from the 134th Judicial District Court Dallas County, Texas ____ RELATOR'S PETITION FOR WRIT OF MANDAMUS ____ FRIEDMAN &

6. Conclusion

RSS/Blog Aggregators can help attorneys make better use of their time by automatically filtering information available online and cutting down on some of the "information overload". Using the right aggregator as a research tool, attorneys can focus on topics they actually care about and get direct access to the information they need to know.

Bonus: A flavor of available (non-legal, non-research) aggregators:

- **AllTop** pulls the top headlines from popular topics on the web, in real time. You can narrow your search by selecting from a list of topics to see selected sources or you can create your own feed.
- **Popurls** pulls in content from a variety of social networks, blogs, and news organizations.

- **The Web List** collects content from a variety of popular news sources. You can customize the order of the content from pre-selected sources.
- **Feedly** allows you to pull content from a wide variety of sources including YouTube channels, Tweets, and keywords. It also has tools for team collaboration and easy sharing.
- **NewsBlur** allows you to read content in its original form. It also allows you to tag stories.
- **Mondaq** hosts content about legal, accounting, regulatory, compliance and commercial issues.

Sources

https://wpmayor.com/6-best-examples-content-aggregator-websites/ (Published Oct. 23, 2018; Visited Dec. 08, 2018).

https://yourbusiness.azcentral.com/list-blog-aggregators-13665.html

https://www.wiyre.com/list-of-blog-aggregator-websites-to-promote-your-blog/

About the Authors

Ronald Chichester is a solo practitioner who specializes in all aspects of law that involve computers and digital networks. He is a past chair of the Computer & Technology and the Business Law Sections of the Texas Bar, and is currently based in Magnolia, Texas.

Lisa M. Angelo is a cyber liability attorney and Certified Information Privacy Manager. Her law practice is focused on advising clients on data privacy, cyber insurance, technology contracts, and other matters related to cyber and technology law.

A Lawyer’s Genetic Fingerprinting Primer

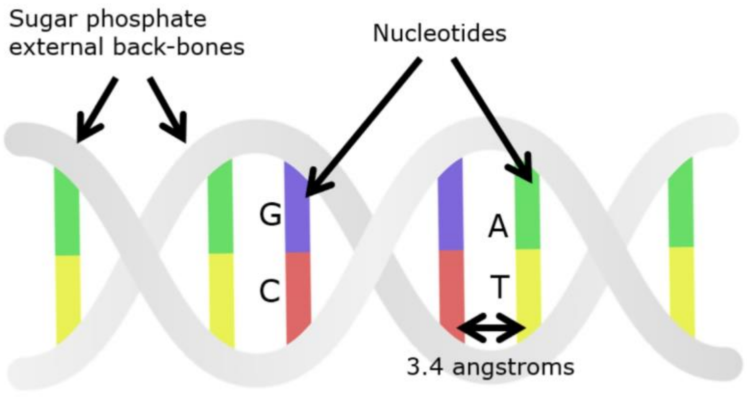
By Pierre Grosdidier

Is genetic fingerprinting the complete de facto surrender of highly personal medical information, or is it an innocuous and clever way of nabbing criminals and exonerating innocents? This primer explains how genetic fingerprinting works so you can develop your own lawyerly answer to this question and inform your clients accordingly. This article focuses on genetic fingerprinting as implemented in government-maintained DNA databases, such as the FBI’s Combined DNA Index System (CODIS).

As Watson and Crick cleverly demonstrated, our genetic information is stored in double-stranded molecular helixes called chromosomes. Humans have 23 chromosome pairs, for a total of 46. We inherit one chromosome in each pair from our father, and the other from our mother. Everybody has chromosomes: fruit flies have four pairs; yeast 16 pairs, chimps 24, armadillos 32, and red king crabs 104.[1]

Each strand in each double helix is comprised of a series of four possible molecules called nucleotides, with the esoteric names cytosine (“C”), guanine (“G”), adenine (“A”), and thymine (“T”). Each strand is a long string of combinations of these four molecules held together by an external back-bone of sugar phosphate molecules that we can safely ignore in this primer (Figure 1). The nucleotides are paired opposite each other in the double helix and, for chemical reasons that also do not matter here, A is always paired opposite T and G is always paired opposite C. Therefore, if you know one strand, you can trivially deduce the other.

Figure 1. The double helix and nucleotide pairs.



[1] *See* https://en.wikipedia.org/wiki/List_of_organisms_by_chromosome_count.

There are approximately 3.2 billion nucleotide pairs in the human genome distributed among our 46 chromosomes.[2] The distance between each nucleotide pair is 3.4 angstroms (10^{-8} cm). Therefore, the chromosomes would measure about 109 cm in length if they were all lined up one after the other like a dashed line.

The nucleotides are not aligned randomly along the chromosomes—far from it. The *sequence* of the nucleotides is what makes the genetic code. A gene is a particular sequence of nucleotides, like AGC or ACC, separated from other genes by other "flanking" sequences that mean "begin" and "end." This article provides a good analogy. The article means nothing if you place all its letters and punctuation marks in a box, shake them like in a game of Scrabble, and align them one after the other as they are randomly plucked from the box. But, if you align the letters and punctuation in order as in this article, you have information. So it is with nucleotides. You can even analogize the spaces between the words to the "flanking" sequences between genes.

Most of the human genome is the same for all humans, with minor variations. The human genome has been sequenced and geneticists have identified some 20,400 protein-coding genes, meaning that they know what the gene does and where and on which chromosome it is located.[3] This information means that geneticists know where to look to determine if a patient has a gene mutation that makes the patient prone to a particular disease. But, that sort of very personal information is *not* what is loaded in DNA fingerprinting databases.

Geneticists have found that some areas of the genome contain specific sequences of nucleotides that repeat themselves, which they have called short tandem repeats ("STR").[4] For example, the sequence TCAT is a tetranucleotide ("tetra" for "four") STR that might repeat itself nine times at a particular location (a locus, plural loci) on a specific chromosome, say chromosome 11, as follows:

. . . ATACTTGAC**TCATTCATTCATTCATTCATTCATTCATTCATTCAT**TCGATCCATA . . .

In this example, the underlined bold letters represent the nine STRs and the regular letters represent the flanking regions. Geneticists have discovered many such STRs at many loci in the genome. Importantly, the number of times these STRs repeat themselves varies significantly among humans, for reasons that need not concern us. And, absent a mutation, the numbers of

[2] https://en.wikipedia.org/wiki/Introduction_to_genetics.

[3] https://en.wikipedia.org/wiki/Human_genome.

[4] STRs are also called "microsatellites" or "simple sequence repeats."

repeats are inherited from the parents. As noted, a person has two chromosomes 11, one inherited from each parent. That person may have five TCAT STRs on one chromosome 11, and nine on the other. This information is reported as "5, 9" for this STR locus. Statistically, because STRs vary significantly from one person to the next, only a subset of people can claim "5, 9" for their TCAT locus. This last observation should give you a hint of where this primer is going.

Geneticists at the FBI selected 20 STR loci that technicians can measure with relative ease[5] and that, in the current state of knowledge, do not code for proteins, which means that these loci cannot disclose a person's medical information, at least for now.[6] These 20 loci and the chromosomes on which they are located are listed in Table 1.[7]

Table 1. The 20 STRs used in genetic fingerprinting.

STR loci	Chromosome	STR loci	Chromosome	STR loci	Chromosome
CSF1PO	5	D18S51	18	D2S441*	2
D3S1358	3	D21S11	21	D2S1338*	2
D5S818	5	FGA	4	D10S1248*	10
D7S820	7	TH01	11	D12S391*	12
D8S1179	8	TPOX	2	D19S433*	19
D13S317	13	vWA	12	D22S1045*	22
D16S539	16	D1S1656*	1	AMEL**	X, Y

* STR added after January 1, 2017.

** Amelogenin, for sex typing.

The genetic fingerprint of a person, referred to as the person's "DNA profile" is reported in genetic fingerprinting databases as the number of repeats for each STR locus, as shown in Table 2 (columns 1 and 2). The only other reported information in the databases are the sample number, the analyzing lab number, and the technician number (not shown here). No offender personal information is stored in the databases, and no medical information can be inferred about the suspect because these 20 loci are not known to code for proteins, *i.e.*, they do not appear to accomplish anything.

[5] With a relatively inexpensive DNA testing kit.

[6] Until January 1, 2017, genetic fingerprinting databases recorded information for just 13 loci.

[7] Europe uses 12 loci and the UK 17, some of which overlap with those used in the U.S.

Table 2. Sample DNA profiles for a known offender and a crime scene sample.*

STR loci	Suspect's DNA profile	Crime scene DNA profile		Probability of a match
		Perfect match	Partial match	
CSF1PO	11, 15	11, 15	11	0.15
D3S1358	14, 17	14, 17	14, 17	0.03
D5S818	10, 11	10, 11	11	0.09
D7S820	9, 14	9, 14	–	0.21
D8S1179	14, 16	14, 16	14, 16	0.12
D13S317	8, 12	8, 12	8	0.06
D16S539	9, 11	9, 11	9, 11	0.07
D18S51	12, 14	12, 14	12	0.11
D21S11	25, 30	25, 30	25, 30	0.32
FGA	21, 22	21, 22	22	0.02
TH01	6, 9	6, 9	–	0.11
TPOX	8, 11	8, 11	8	0.21
vWA	15,16	15,16	15,16	0.18
D1S1656	5, 10	5, 10	10	0.08
D2S441	30, 35	30, 35	30	0.27
D2S1338	14, 15	14, 15	14, 15	0.05
D10S1248	11, 11	11, 11	11	0.12
D12S391	9, 15	9, 15	9, 15	0.22
D19S433	6, 9	6, 9	6, 9	0.13
D22S1045	25, 35	25, 35	35	0.06
AMEL	XY	XY	XY	2.79×10^{-20}

* This DNA profile and its associated probabilities are purely illustrative and not actual values.

In a police investigation, the DNA profile of a suspect (Table 2, column 2) is compared to the DNA profile of a sample taken from the crime scene (Table 2, column 3). DNA profiles of new suspects can also be compared to old DNA profiles kept in databases (like CODIS) to see if the suspect can be tied to another case—even a “cold” one that is decades old. A perfect match occurs when all the STR counts are the same (Table 2, columns 2 and 3). In some cases, the

DNA collected at the crime scene is degraded and only a partial match is possible because not all STRs can be counted (Table 2, column 4).

It is possible to calculate the probability of a match. For each STR locus, geneticists can calculate the probability that a random person has the same pair of repeats as a suspect (Table 2, column 5). These calculations are non-trivial and consider several factors, including the suspect's ethnicity.[8] For example, in Table 2, the probability that a random person other than the suspect also has repeats "11, 15" at the CSF1PO locus was calculated at 0.15, or 15%. For the D3S1358 locus and repeats "14, 17", this probability was calculated at 0.03, or 3%. Therefore, because there is no reason to expect a cross-correlation between the two loci, the probability that another random person has both locus repeats identical to the suspect's is $0.15 \times 0.03 = 0.0045$ or 0.45%. And, by the same logic, the probability that another random person has all 20 loci repeats identical to those of the suspect is the product of all the probabilities or 2.79×10^{-20}, or 0.000 000 000 000 000 002 79%. That is 2.79 billionth of a billionth percent. The implication is that if the DNA profile of a suspect matches that found at a crime scene, then the two DNA profiles are from the same person—because the existence of another person with the same DNA profile is so remotely unlikely. Other circumstantial evidence, such as the suspect's presence near the crime scene, or his or her knowledge of the victim, can clinch the case. It is easy to see why the police can be so confident when they nab a suspect via genetic fingerprinting.

Returning to the question at the start of this article, genetic fingerprinting unquestionably raises a host of ethical questions, like how willingly should a person volunteer to publish his or her DNA profile, for what level of criminal activity should authorities forcibly take DNA samples from suspects, what happens to the DNA profile of suspects who are cleared, and how long should DNA profiles be retained in databases? But, barring further developments to the contrary, DNA profiles are barren of medical information and should not raise objections on that basis. In a sense, they are like a person's hair or eye color, fingerprints, or tattoos: physical attributes that are very convenient for identification, but unrevealing about the person's health or medical condition.[9]

[8] The probabilities shown in Table 2 are all invented for illustrative purpose.

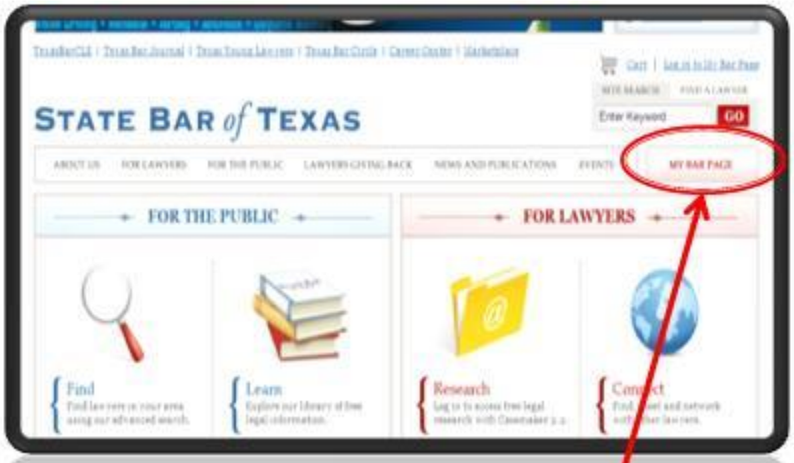
[9] The interested reader wanting to dig further will find ample material on Internet and Wikipedia.org. I enjoyed reading the following article for its depth and clarity: Karen Noorgard, Forensic, DNA Fingerprinting, and CODIS, Nature Education 1(1):35 (2008).

About the Author

Pierre Grosdidier is Counsel in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. Pierre divides his practice between construction litigation and construction contract drafting. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), and the State Bar of Texas Computer & Technology Section Webmaster and Circuits eJournal Co-Editor for 2018-19.

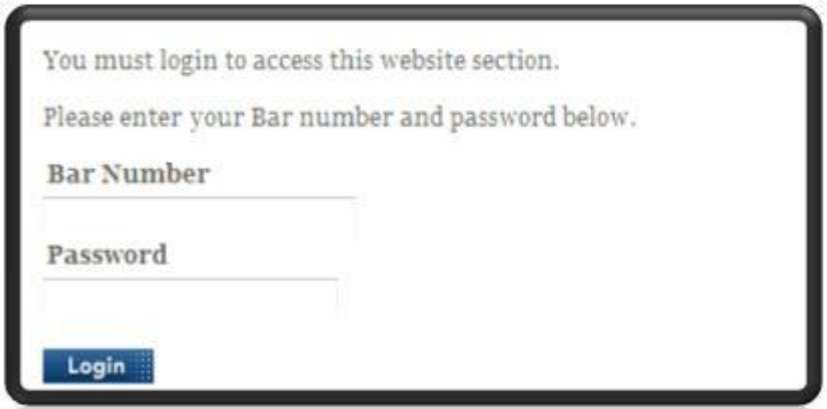
How to Join the State Bar of Texas Computer & Technology Section

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.

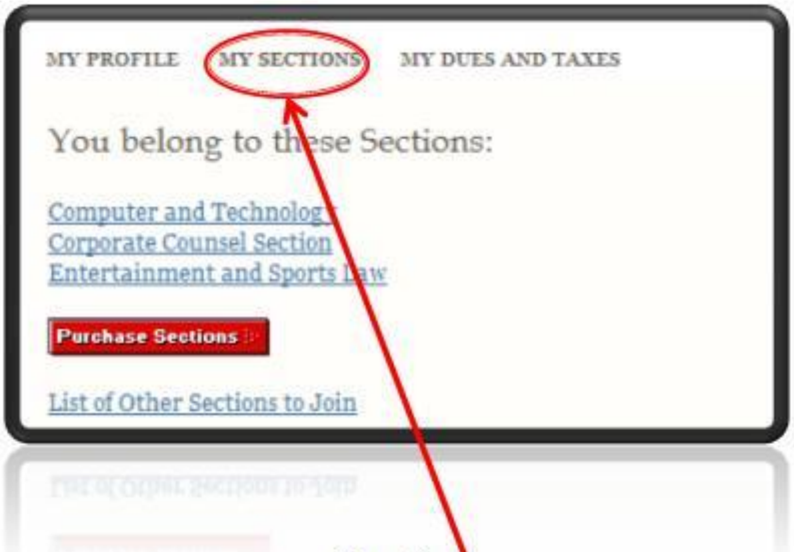
Bar Number

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

Sammy Ford IV – Houston – Chair
John Browning – Dallas – Chair-Elect
Shawn Tuma, Fort Worth – Treasurer
Elizabeth Rogers – Austin – Secretary
Michael Curran – Austin – Past Chair

Webmaster

Pierre Grosdidier – Houston

Circuits Co-Editors

Pierre Grosdidier – Houston
Kristen Knauf – Dallas

Term Expiring 2021

Chris Krupa Downs – Plano
Seth Jaffe – Houston
Honorable Emily Miskel – Collin County
William Smith – Austin

Term Expiring 2020

Lisa Angelo – Houston
Eddie Block – Austin
Kristen Knauf – Dallas
Rick Robertson – Plano

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

2017-2018: Michael Curran
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