COMPUTER AND TECHNOLOGY SECTION

Circuits

e-Journal of the Computer & Technology Section
of the State Bar of Texas
February 2022

Table of Contents

Featured Articles

Short Circuits

Table of Contents

Feature Articles:-

Short Circuits:-

Message from the Chair

By Elizabeth C. Rogers

On behalf of the Council of the Computer and Technology Law Section of the State Bar of Texas, I hope this issue of Circuits finds you and your families healthy. The past two bar years have been especially challenging due to the COVID-19 restrictions we have seen nationwide. We are disappointed that, due to the many "social" distancing mandates, our interaction and engagement with each other and with our section members has resulted in not only social distancing but also "professional" distancing.

As you may know, the Council has announced that it is postponing the 5th Annual "And Justice for All" CLE from December 16, 2021 to February 11, 2022. We made this decision to avoid the costs of renting a hotel conference room facility and AV rental due to the fact that the State Bar Building closed in December due to COVID-19 precautions. Unfortunately, we are not going to be able to have the CLE in person, but we are excited that it will be a live Zoom webinar from 9:00 a.m. to 2:15 p.m. CST on Friday, February 11th. For more information or to register, click here.

Additionally, we are carefully reviewing our options for our annual retreat in April of 2022. We made the tough decision to cancel our retreats in April 2020 and April 2021 due to COVID-19 travel and lodging restrictions, and out of concern for the health and safety of our Council Members. Our annual retreat is usually built around a theme that will enlighten and educate all council members about a trending issue involving legal technology or legal technology resources that we can, in turn, pass on to our members and the greater Bar membership. We are hopeful that we will be traveling to Silicon Valley to meet with and to explore strategic relationships with several thought-leaders in technology innovations in academia and inside of the technology corporate giants.

Meanwhile, looking back over 2021, notwithstanding the challenges of the lockdown and quarantines, our individual council members and our council as a whole experienced a productive year with a few noteworthy accomplishments. John Browning, one of our immediate past Presidents and one of the most prolific writers of all currently licensed Texas attorneys, received the Maurice Merrill Golden Quill Award for the author of the best written article published this year in the Oklahoma Bar Journal. Additionally, the Texas Bar Foundation recognized the Honorable Fifth Circuit Judge – and one of our Council's esteemed judicial members – with the Samuel Pessarra Outstanding Jurist Award. Finally, our current Membership

Chair, Lisa Angelo, was recognized by the Houston Infraguard Members Alliance with the 2021 Outstanding Achievement Award – Lifetime Achievement Award. Incidentally, Lisa Angelo also received a Chair's award by immediate past President, Shawn Tuma, for her contributions to the Council in the bar year of 2020 and 2021 as did Council member Ron Chichester, for his contributions to our website.

Since the beginning of the Bar year in June of 2021, we have held two Council meetings. In September, under the leadership of our Social Media Chair, Alex Shahrestani, we passed a new Social Media Conduct and Content Policy and announced that one of our newest Council Members, Will Trevino, will be the 2021-2022 Bar Year Chair of our Techbytes Task Force. Please reach out to either Alex or Will if you have any content you'd like our Council to post on your behalf or if you have any ideas for the filming of a "Techbyte" that will benefit our membership. Our September meeting guest speaker was Representative Rep. Gio Capriglione who provided us with an informative update about the most recent cybersecurity legislation that took effect on September 1, 2021, as a result of Rep. Capriglione's determined and effective guidance.

At our meeting held on December 16, 2021, we passed a motion that requires all current and new Council Members to contribute at least 1 full *Circuits* article (500-1500 words) or two *Short Circuits* (250-500 words) per year. This should help us publish more diversity of content from a greater diversity of contributors. We also welcome articles from our membership. The content does not have to be original to be published and can be re-purposed from other publications who give permission. If you would like to be published, please contact Circuits@sbot.org. Another shorter version of the *Circuits* will be published in March of 2022, so please send in your contributions! We also welcome your posts on any of our social media platforms, including Twitter, LinkedIn, Facebook and Instagram. Also, please like these platforms if you have not already to stay up to date with the latest computer and technology legal developments.

The final noteworthy update is that Mark Unger, a past President and ex-officio member of the Council, announced that our Section App has been updated to include all legislation passed by the 87th Texas Legislature in 2021. Shortly before adjourning, we were honored to receive a visit from current State Bar of Texas President Sylvia Borunda Firth, who provided a timely update of the state of the Bar.

In closing, please know how much we value your membership in the Computer & Technology Section of the State Bar of Texas. We welcome your feedback about what are your expectations

and what we can do to improve your benefits at any point in time. We also welcome your participation on any of our working groups or committees without needing to be a member of the Council. Please reach out to me if you have any interest or thoughts. Until our next issue, please have a safe and joy-filled holiday break with your friends and family! And, early happy 2022!!

Respectfully,

Elizabeth C. Rogers
2021-2022 Chair
Computer & Technology Section
State Bar of Texas

Letter from the Editor

By Matthew Murrell

Welcome to the first issue of *Circuits* for 2022! As I write this letter in mid-December 2021, the State of Texas Department of Health and Human Services reports that there have been 3.6 million confirmed cases of COVID-19 in Texas, with an additional three-quarters of a million probable cases since the pandemic began.

While it remains to be seen whether we're approaching the closing chapter of the pandemic, one thing is certain: the pandemic has indelibly changed the intersection of law and technology. The pandemic has not only spurred the use of technology in the practice of law, but it has also created novel questions regarding substantive legal issues involving technology. In this issue, our authors explore the ever-expanding scope of law and technology.

Our first and second articles are by Ron Chichester and explore the transition of entities and contracts into the virtual sphere. The first article, *How Do You Incorporate an Entirely Digital Corporation*, addresses companies that are almost exclusively virtual because they rely heavily (or totally) on blockchain technology. The article offers excellent primers on the basics of virtual companies, including blockchains, smart contracts, and distributed autonomous organizations (DAO), before taking a deep dive into how such entities are structured and may be regulated. The second article, *Tezos and SmartPy: Accessible Smart Contracts on an Upgradeable Platform*, plumbs the depths of smart contracts used by such companies, exploring the key differences between smart contracts—which are a creature of software—and traditional contracts.

The third article, *Digital Zoom* by Anthony Ng, is ripped straight from recent headlines. Like a growing number of criminal trials, the trial of Kyle Rittenhouse in Wisconsin featured digital-video evidence of the alleged crime. When the prosecutors wanted to "zoom in" on—in CSI lingo, "enhance"—a portion of the video and play it for the jury, the issue arose what exactly happens when zoom is engaged on a digital video. Anthony's article dives into that issue.

The fourth and fifth articles are by Pierre Grosdidier and explore recent court decisions regarding the use of cameras by police departments. The fourth article, *Big Brother-Style Aerial Surveillance Requires a Warrant,* analyzes the successful challenge in the Fourth Circuit to the Baltimore Police Department's use of airplanes to create gigantic aerial photographs of Baltimore ("32 square miles per image per second"). The fifth article, *A Body-Worn Camera*

Does Not Dispense the Need for a Warrant, examines the scope of how footage recorded by body cameras worn by police officers may be used after the fact.

This issue also features two *Short Circuits*. In the first, Michael Curran explores five take-aways from President Biden's 2020 Executive Order on cybersecurity. In the second, Pierre Grosdidier examines the Supreme Court's decision in *Facebook v. Duguid*, which has the potential to substantially alter litigation regarding the Telephone Consumer Protection Act.

I hope you enjoy the content in this issue. If you have any questions about the use of technology in the practice of law, note that the Computer and Technology Section has a lot of tools available to help us lawyers remain productive remotely in practice. Do not hesitate to contact us through our section administrator at admin@sbot.org if you have questions about technology and the law or would like to contribute to a future issue of *Circuits*.

Kind Regards,
Matthew Murrell, Editor

How Do You Incorporate an Entirely Digital Corporation?

By Ronald Chichester

1. Abstract

This paper describes what attorneys need to know about incorporating companies that rely heavily – if not exclusively – on blockchains. Because technology is central to this topic, references will be provided for a brief introduction to: cryptocurrencies, blockchains (which is the underlying technology to cryptocurrencies), smart contracts, and distributed autonomous organizations. Finally, this paper will discuss the peculiar requirements for incorporating a blockchain-based company.

2. What is a Cryptocurrency?

Most people's introduction to blockchains comes from their experiences with cryptocurrencies. According to Forbes, a "[c]ryptocurrency is decentralized digital money, based on blockchain technology.[1] Examples of cryptocurrencies include Bitcoin[2] and Ethereum.[3] Ethereum has the added benefit of executing code that controls digital value.[4] Essentially, cryptocurrencies enact a different trust paradigm, wherein middle*men* (banks and governments) are replaced by middle*things* (computers and networks). Cryptocurrencies rely on three major elements: peer-to-peer networking,[5] encryption,[6] and game theory.[7] As with most national currencies, most cryptocurrencies are fiat, in that they are not backed by some finite commodity, such as gold. Cryptocurrencies are essential for monetary transactions involving blockchain-based companies. Once companies and individuals have accounts (addresses) on a particular cryptocurrency, that company or individual may conduct transactions with any other individual

---

1 Kate Ashford and John Schmidt, *What is Cryptocurrency?*, Forbes Advisor (December 18, 2020) https://www.forbes.com/advisor/investing/what-is-cryptocurrency/

2 https://bitcoin.org/en/ ("Bitcoin is an innovative payment network and a new kind of money.")

3 https://ethereum.org/en/ ("Ethereum is a global, open-source platform for decentralized applications.)

4 *Ibid.*

5 *See, e.g.,* Peer-to-peer, https://en.wikipedia.org/wiki/Peer-to-peer

6 *See, e.g.,* Encryption, https://en.wikipedia.org/wiki/Encryption

7 *See, e.g.,* Game theory, https://en.wikipedia.org/wiki/Game_theory

or company that has access to the same cryptocurrency. There are also exchanges for cryptocurrencies, such as Binance.[8]

3. What is a Blockchain?

The underlying technology used to implement a cryptocurrency is called a *blockchain*. A blockchain is a computerized ledger that is suitable for use within an organization, or within multiple organizations and individuals. Note, in many jurisdictions, blockchains are often referred to (generically) as *distributed ledgers*.

Blockchains have two or more physical components: at least one *node* and a way to get information to/from the nodes. Each node in the blockchain is running identical software precisely so it can process transactions like every other node. The software can be open source or it can be proprietary, but it must be identical to every node on the blockchain.[9] The software running on the node validates (or not) the transactions. If there is more than one node, they are typically connected to each other by a peer-to-peer network. Users place their transactions on the peer-to-peer network, and the nodes race to validate it. If validated, the transaction is encrypted and the encrypted record is inserted into a block. Then the block is cryptographically *hashed*[10] and that hash value can be shared with the other nodes to ensure that all of the nodes agree. Typically, once at least half the nodes agree on the validity of the transaction, then the transaction is considered validated. Each block is then hashed with all previous blocks to form a chain of blocks, hence the name blockchain. Generally, if a node's hash doesn't comport with the other nodes, then that node replicates the blocks from the other nodes to bring itself into compliance. There is an incentive for the nodes to comport with each other. If a node is not compliant, it cannot be trusted to execute further transactions, rendering that node useless to the blockchain, and the owner of the node precluded from remuneration for hosting that node.

While there is no standard architecture for blockchains, in general, most are considered either *public* or *private*. Private blockchains are controlled by a single entity and are generally used to facilitate transactions between a small group of trusted entities. Public blockchains, however, are available to the public for transactions between any set of companies or individuals that

---

[8] Binance.com, https://www.binance.com/en

[9] For example, Bitcoin node software is open source, and is available at: https://bitcoin.org/en/full-node

[10] *See, e.g.,* Cryptographic hash function, Wikipedia, https://en.wikipedia.org/wiki/Cryptographic_hash_function

don't need to trust each other. Bitcoin is an example of a cryptocurrency that is on a public blockchain.

The design of the blockchain is vital to the purpose of the resulting transactions. While the basic design of blockchains *can* be robust and secure, the design decisions enacted can affect on *how* robust and secure the resulting blockchain will be. The linchpin for blockchain design is the number (and ownership) of the nodes. The greater the number of nodes (and owners), the more robust the blockchain because the more difficult it is to validate an improper transaction. Unfortunately, this design makes it difficult to update the software for the nodes, and is as intended. However, updates and/or hostile takeovers of a blockchain are possible, and that process is called a *fork*.[11] How easy (or difficult) it is to fork a particular blockchain design is an important risk factor for investors.

A truly detailed introduction to blockchains is outside the scope of this article. Fortunately, there are many good introductions to blockchain on the Web and YouTube, and I commend your attention to those resources.[12] For a detailed explanation of the trust paradigm (and legal implications thereof) made possible by blockchains, see the seminal book on blockchains and resulting trust paradigms by Kevin Werbach.[13]

4. What is a Smart Contract?

"A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible."[14] The code can run on a non-proprietary cryptocurrency blockchain, such as Ethereum,[15] or on a private blockchain. When a software application is implemented on a distributed blockchain, that application is called a

---

[11] *See, e.g.,* Coin Idol*, Definition of a Cryptocurrency Fork; Why are They Necessary?*, Coin Idol.com (February 9, 2020), https://coinidol.com/definition-cryptocurrency-fork/

[12] *See, e.g.,* How does a blockchain work - Simply Explained, https://www.youtube.com/watch?v=SSo_EIwHSd4

[13] Kevin Werbach, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST, (Massachusetts Institute of Technology, 2018).

[14] Jake Frankenfield, *What is a Smart Contract?*, Invetopedia (October 8, 2019) https://www.investopedia.com/terms/s/smart-contracts.asp. Smart contracts were invented by Nick Szabo in 1994. *See*, Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, (1996) https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[15] *Supra*, note 4.

"dapp." and a smart contract is an example of a dapp.[16] Incidentally, private blockchains are easy to set up. Much of the software is open source[17] and readily available. In fact, you can set up your own Ethereum blockchain for development purposes using software such as Truffle and Ganache.[18] This means that the cost of entry for a cryptocurrency is very low, which accounts for their proliferation.

When two companies consummate a smart contract, the software code that describes the terms of the contract are placed (instantiated) onto, for example, the Ethereum blockchain. The goal of a smart contract is to automate the compliance of the terms as much as possible, and not to rely on human interaction or intervention. To that end, reliance is placed on electronic devices that are often part of the "Internet of Things" ("IoS"), which are capable of conducting transactions on the same blockchain as the smart contract. For example, an automaker could contract for 500,000 spark plugs from a vendor through a smart contract in Ethereum. The code for the smart contract may expect a signal from an IoT device when an individual spark plug leaves the factory, and trigger a micro-payment to the spark plug manufacturer upon that event with Ether cryptocurrency. Final payment could be made upon detection (by another IoT device) of the delivered spark plug at the automaker's factory. All of the terms of the contract are reflected in the code. All remedies for problems may also be reflected in the code, which thus precludes parole evidence and (most) potential lawsuits. Contractual language can thus be commoditized and thereby reducible to rigid computer code that is known by (and testable by) both parties using an agreed-upon set of code. Workflows that define the process of the contract can be defined in a domain-specific language, such as *Legalese.*[19] Software frameworks, such as Brownie,[20] exist that simplifies the process of drafting and implementing a smart contract.

---

[16] *See, e.g.,* Introduction to Dapps, Ethereum Developer Documentation (January 12, 2021) https://ethereum.org/en/developers/docs/dapps/

[17] For more information about open source software, *see*, https://opensource.org/

[18] CodeOoze, *How to install Truffle and Ganache in Ubuntu 18.04*, CodeOoze.com (February 17, 2019) https://www.codeooze.com/blockchain/ethereum-dev-environment-2019/ Ganache is a quick and easy way to run a personal blockchain for developing and deploying smart contracts. Truffle is used to manage smart contract projects, testing, compiling and migration. *Id.*

[19] https://legalese.com/

[20] Brownie is a Python-based development and testing framework for smart contracts targeting the Ethereum Virtual Machine. https://github.com/iamdefinitelyahuman/brownie-v2 *See also*, Saurav Verma, *Learn the Basics of Brownie*, Better Programming (January 31, 2020) https://medium.com/better-programming/part-1-brownie-smart-contracts-framework-for-ethereum-basics-5efc80205413.

5. What is a Distributed Autonomous Organization ("DAO")?[21]

"With smart contracts, a blockchain network gains the power of automated decision-making and execution."[22] "that capability can be used to create a new algorithmic organizational form: the distributed autonomous organization, or DAO."[23] Under the "nexus of contracts theory" of corporations, a company is nothing more than a set of contracts.[24] Similarly, a set of smart contracts are said to form a DAO.[25] Essentially, "[t]he standard corporate arrangements of equity, debt, and corporate governance can be encoded in a series of smart contracts based on cryptocurrencies."[26]

Examples of DAOs include DAOstack,[27] Jelurdia,[28] MakerDAO,[29] and Moloch DAO.[30] While at the moment, many DAOs are themselves devoted to the automation of DAO-creation, the Moloch DAO is devoted to funding startups that are themselves DAOs. As one might expect,

---

[21] Note, distributed autonomous organizations are also known as decentralized autonomous organizations. The names are synonymous, and both share the same acronym "DAO". For this article, I have adopted the former name.

[22] Werbach, *supra* note 13 at 110.

[23] *Id.*

[24] *See, e.g.,* Ronald F. White, *Nexus of Contracts Theory*, http://faculty.msj.edu/whiter/nexusofcontracts.htm (this articles is taking an economist's view of the theory). *See also,* Soumik Chakroborty, *Corporation As Nexus of Contracts: A Critque*, Academike (December 17, 2014) https://www.lawctopus.com/academike/corporation-nexus-contracts-critique/ ("*The nexus of contracts theory is an idea put forth by a number of economists and legal commentators which asserts that corporations are nothing more than a collection of contracts between different parties – primarily shareholders, directors, employees, suppliers, and customers"). William W. Bratton Jr., Nexus of Contracts Corporation: A Critical Appraisal, 74 Cornell L. Rev. 407 (1989) Available at: http://scholarship.law.cornell.edu/clr/vol74/iss3/1.*

[25] *See, e.g., Distributed autonomous organization*, PlatformValueNow.org (March 2, 2017) https://platformvaluenow.org/signals/distributed-autonomous-organization/ *See also*, Werbach, *supra* note 13, at 110.

[26] Werbach, *supra*, note 13 at 110.

[27] https://daostack.io/ DAOstack is an open source project advancing the technology and adoption of decentralized governance.

[28] https://www.jelurida.com/ Jelurida is a blockchain software company that develops and maintains the Nxt and Ardor blockchains.

[29] https://makerdao.com/en/ MakerDAO is owned by the Maker Foundation. The Maker Foundation is tasked with bootstrapping MakerDAO to fuel growth and drive the organization toward complete decentralization. While the Foundation provided development support through the launch of the cryptocurrency called Multi-Collateral Dai (MCD), it is currently spearheading efforts to decentralize development.

[30] https://www.molochdao.com/

this automation craze has prompted engineers to develop a framework for automating the *generation* of DAOs.[31] This type of automation is expected to increase the number of DAOs, so lawyers should expect to encounter DAO-related legal questions for investors and developers alike.

"As self-executing software running on a distributed blockchain, a DAO need not have any owners in the traditional sense. It simply operates and interacts with the world according to its algorithms."[32] Thus, while a DAO may have human creators, DAOs do not require human employees (or owners), which is a novel concept (and problem) for most jurisdictions. The direction or management of the DAO is typically done in two fashions: algorithmic and AI-assisted. The two fashions are not exclusive, however. Most DAOs are actually hybrids, with some aspects of management being hard-coded in an algorithm, while others are run by AI-trained neural networks. Still other DAOs employ machine learning algorithms to respond to changes in the market. In other words, the DAO can learn "on the job," based on their own perceived experience.

While the hard-coded DAOs are eminently predictable in their behavior, their machine learning cousins are not. The predictability (or not) of DAOs has legal implications. Moreover, the risks (legal and otherwise) of DAOs, while manageable, entail the need for legal advise for investors. Consequently, lawyers need to be conversant in the technology of DAOs in order to advise their clients of the attendant legal implications. No case better illustrates this need for legal *and* technological acumen than one of the first DAOs (confusing called "*The DAO*") which resulted in the infamous Ethereum DAO attack.

"Up until it collapsed, The DAO represented the highest technological achievement – and the coming wave of innovation – that the Ethereum blockchain has enabled."[33] The DAO was the brainchild of Dan Larimer[34] and Vitalik Buterin,[35] the latter being a Russian-Canadian programmer and co-founder of the Ethereum blockchain. The DAO was a crowdfunding service implemented on the Ethereum blockchain.

---

[31] *See, e.g.,* LL-DAO, https://github.com/dOrgTech/LL-DAO

[32] Werbach, *supra*, note 13 at 110.

[33] Daniel Kuhn, *Did Ethereum Learn Anything From the $55M DAO Attack?*, Coindesk (September 20, 2020) https://www.coindesk.com/ethereum-learn-dao-attack

[34] *See, e.g.,* Dan Larimer, Steem.Center https://www.steem.center/index.php?title=Dan_Larimer

[35] *See, e.g.,* Vitalik Buterin, Wikipedia, https://en.wikipedia.org/wiki/Vitalik_Buterin

> "The DAO, which got that name for being the first encoded version of the concept, was the proving ground that the disruptive world of venture capitalism could itself be disrupted. Approximately $150 million in ether was contributed to the project, and more than 50 projects were teed up to possibly be funded by a smart contract that no one person owned."[36]

Once created, The DAO was attacked. Hackers detected a vulnerability in the code making up The DAO, and exploited it. They got away with millions of dollars in cryptocurrency. Worse, copycats appeared and even more cryptocurrency was lost. "Investors withdrew their funds, a 'dark DAO' was spun up to protect the remaining and a serious debate raged over when it might be appropriate to hard fork or roll back events on a blockchain."[37] In the aftermath, market exuberance and lack of attention to security were blamed for the fiasco. For the developer community, it was a hard lesson. Fortunately, the security issues were surmountable, so the overall assessment of the technology remained buoyant. For the investment community, The DAO debacle was an expensive lesson, and demonstrated the need to limit risk while the developers sorted out the details.

6. Business Organizations for Blockchain-Oriented Companies

Several states (such as Delaware[38]) expressly allow the use of blockchains for corporate functions within a standard corporation. However, entrepreneurs determined that a specialized business entity was needed to facilitate the development and implementation of DAOs. That need is particularly acute because DAOs can be fitted with artificial intelligence ("AI") that can – without human interaction – modify the DAOs business model, or develop other business models and pursue different business goals than were first envisioned by its human creators.[39]

---

[36] Kuhn, *supra,* note 33.

[37] *Id.*

[38] *See, e.g.*, Wonnie Song, *Bullish On Blockchain: Examining Delaware's Approach To Distributed Ledger Technology In Corporate Governance Law And Beyond*, Harvard Bus. L. Rev., (2017) Online at: https://www.hblr.org//wp-content/uploads/sites/18/2018/01/Bullish-on-Blockchain-Examining-Delaware%E2%80%99s-Approach-to-Distributed-Ledger-Technology-in-Corporate-Governance-Law-and-Beyond.pdf

[39] *See, e.g.,* Prashant Ram, *The implications of AI on the Blockchain*, Hackernoon (July 24, 2018) https://hackernoon.com/the-distributed-autonomous-organization-dao-and-how-blockchain-ai-can-take-over-the-network-17a51f099d0f *But see,* Werbach, *supra*, note 13 at 110 ("Trusting an AI-trained system, therefore, adds another degree of risk over trusting a system based on hard-coded algorithms."). *See also,* Alexandre Gonfalonieri, *Why Building an AI Decentralized Autonomous Organization (AI DAO): Why most traditional business organizations are in danger (Business models, AI agents, etc.,* Towards Data Science (June 29, 2020) https://towardsdatascience.com/why-building-

Because the developers and owners of the DAO cannot predict what the DAO's AI will do, they understandably wish to limit their liability while still be able to profit from the DAO.

In 2018, Vermont became was the first state to enact a specific business organization type in 2018, namely a blockchain-based L.L.C.[40] Another state, Wyoming,[41] followed Vermont's lead and has enacted a new corporate form – the decentralized autonomous organization – that is tailored to companies making heavy (if not exclusive) use of blockchains. While the Vermont statute does not require the BBLLC to be a DAO, the Wyoming statute presumes the form of a DAO, with the blockchain being a necessary ancillary. In contrast, the Vermont BBLLC merely requires that a blockchain make up some particular aspect of the company, so a DAO can fit within the rubric of a Vermont BBLLC.

7. Example: Vermont's BBLLC Statute

Vermont's blockchain-based limited liability corporation ("BBLLC") statute is under Title 11, §§ 4171-4176.[42] Essentially, the BBLLC is just a regular LLC with some added requirements that are peculiar to DAOs. The statutes states that the "BBLLC may provide for its governance, in whole or in part, through blockchain technology."[43] In Vermont, the company must specify, in its articles of incorporation, that it has elected to be a BBLLC,[44] and subsection (2) of § 4173 includes six other requirements:

> (A) provide a summary description of the mission or purpose of the BBLLC;[45]

---

an-ai-decentralized-autonomous-organization-ai-dao-85d018700e1a; Trent McConaghy, *Artificial Intelligence (AI) DAOs (decentralized autonomous organizations)* BigchainDB (April 19, 2017) https://www.slideshare.net/BigchainDB/artificial-intelligence-ai-daos-decentralised-autonomous-organisations-bigchaindb-ipdb-meetup-4-april-05-2017; SimoneSays, *How to Create the Future of Decentralized Autonomous Organizations* SingularityNET (December 1, 2017) https://blog.singularitynet.io/how-to-create-the-future-of-decentralized-autonomous-organizations-7919d4e5ce36; and S. Ponomarev and A.E. Voronkov, *Multi-Agent systems and decentralized artificial superintelligence*, Arxiv.org, https://arxiv.org/ftp/arxiv/papers/1702/1702.08529.pdf

[40] *See* 11 V.S.A. § 4173.

[41] *See*, Wyoming Senate Bill 38 (2021) https://wyoleg.gov/Legislation/2021/SF0038, which went into effect on July 1, 2021, and created sections 17-31-101 through 17-31-116 of Wyoming Statutes.

[42] 11 V.S.A. § 4171 *et. seq.*

[43] 11 V.S.A. § 4173(1).

[44] 11 V.S.A. § 4172.

[45] 11 V.S.A. § 4173(1)(A).

(B) specify whether the underlying blockchain "will be fully decentralized or partially decentralized" and whether the blockchain "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;"[46]

(C) "adopt voting procedures, which may include smart contracts" that are implemented on the blockchain to address forking,[47] changes to the operating agreement of the BBLLC,[48] and "any other matter of governance or activities within the purpose of the BBLLC;"[49]

(D) adopt protocols to respond to system security breaches or other unauthorized actions that affect the integrity of the blockchain technology utilized by the BBLLC;[50]

(E) 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;[51] and

(F) 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.[52]

The Vermont statute makes special mention of *members* and *managers*. However, those terms don't have any special meaning within the ambit of the BBLLC statute, and thus have the same meaning as for other LLCs. § 4174 expressly states that members and managers can have multiple roles within the BBLLC, "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."[53] This remains true regardless of the location of that person.[54]

---

[46] 11 V.S.A. § 4173(1)(B).
[47] 11 V.S.A. § 4173(1)(C)(i).
[48] 11 V.S.A. § 4173(1)(C)(ii).
[49] 11 V.S.A. § 4173(1)(C)(iii).
[50] 11 V.S.A. § 4173(1)(D).
[51] 11 V.S.A. § 4173(1)(E).
[52] 11 V.S.A. § 4173(1)(F).
[53] 11 V.S.A. § 4174(a).
[54] 11 V.S.A. § 4174(b).

Finally, the Vermont BBLLC law has a very important provision regarding the technological structure of the company. § 4175 requires that, in the governance of the corporation, the company must "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."[55]

Clearly the authors of the Vermont BBLLC law were concerned, for investor's sake, about the design of the blockchain, as reflected in subsections (B), (C) and (D). It should be noted, however, that Vermont law did not directly affect the potential of AI morphing the operation of the DAO. However, Vermont made a very clever caveat provision that should apply in situations with AI-in-command, namely § 4175(2), which requires "in accordance with any procedure specified pursuant to section 4173 of this title, modify the consensus process, requirements, processes, and procedures, or substitute a new consensus process, requirements, processes, or procedures that comply with the requirements of law and the governance provisions of the BBLLC."[56] In other words, if the AI (or humans) morph the company's business model and/or governance model, an amendment to the articles of incorporation is required. In any case, lawyers who are going to advise clients as to *how* to characterize the blockchain and operation, as required in subsections (B), (C) and (D) of § 4173 will need to be versed in the technology.

8. Wyoming's Distributed Autonomous Organization Statute

Wyoming's DAO corporate form (hereinafter "SF 38")[57] differs from Vermont's law in several ways. SF 38 applies LLC status to a DAO, rather than focusing on the use of a blockchain within an LLC as in Vermont. Under SF 38, the company is an LLC that elects a "status" as a "decentralized autonomous organization." Further in contrast to Vermont, a Wyoming company that is already an LLC could "convert" to claim DAO status by amending its articles of organization to include the required language.[58] Interestingly, SF 38 requires that the status of the DAO be included within the name of the company in one of three ways: "DAO", "LAO", or "DAO LLC."[59] Another important requirement in SF 38 is that a DAO must, within the articles of

---

[55] 11 V.S.A. § 4175(1).

[56] 11 V.S.A. § 4175(2).

[57] Wyoming Senate File 0038, which is available at: https://wyoleg.gov/Legislation/2021/SF0038.

[58] *Id.*

[59] *Id.*

incorporation, define the company as *either* a member managed DAO, or an algorithmically manage DAO (and the member managed selection is the default).[60]

There are some additional requirements under Wyoming SF 38, namely the requirement that "the articles of organization shall include a publicly available identifier of any smart contract directly used to manage, facilitate or operate the decentralized autonomous organization."[61] How that would work in practice is an open question. As alluded to with the Vermont law, the Wyoming legislation would require amendment of the articles of incorporation if the DAO's smart contracts are "updated or changed."[62] Presumably, that change could be accomplished by a human, or by AI-enhanced code, although the proposed legislation was silent as to that issue.

9. The SEC's Cautionary Role

On July 25, 2017, the Securities and Exchange Commission issued an investigative report "cautioning market participants that offers and sales of digital assets by "virtual" organizations are subject to the requirements of the federal securities laws."[63] Specifically, the SEC cited its own Report of Investigation 34-81207,[64] wherein tokens offered and sold by a "virtual" organization known as "The DAO"[65] were securities and therefore subject to the federal securities laws.[66] The report notes that, despite what happened specifically to "The DAO," the usual registration requirements for securities still applied to DAOs in general.[67] In short, the *Howey*[68] rule applies to DAOs.

---

60 *Id.*

61 *Id.*

62 *Id.*

63 SEC Issues Investigative Report Concluding DOA Tokens, a Digital Asset, Were Securities, Securities and Exchange Commission News Release 2017-131, available at: https://www.sec.gov/news/press-release/2017-131.

64 See SEC Report of Investigation Release No. 81207 (July 25, 2017), available at https://www.sec.gov/litigation/investreport/34-81207.pdf

65 For more about "The DAO", *see, e.g.,* "Slock.it", Gripeo.com (November 3, 2020), available at: https://www.gripeo.com/slock-it/

66 *Supra*, note 64. *See also*, Tiffany L. Minks, ETHEREUM AND THE SEC: WHY MOST DISTRIBUTED AUTONOMOUS ORGANIZATIONS ARE SUBJECT TO THE REGISTRATION REQUIREMENTS OF THE ORGANIZATIONS ARE SUBJECT TO THE REGISTRATION REQUIREMENTS OF THE SECURITIES ACT OF 1933 AND A PROPOSAL FOR NEW REGULATION SECURITIES ACT OF 1933 AND A PROPOSAL FOR NEW REGULATION, 5 Tex. A&M L. Rev. 405 (May 1, 2018), available at: https://scholarship.law.tamu.edu/cgi/viewcontent.cgi?article=1138&context=lawreview

67 Tiffany, *supra,* note 64 at 426.

68 *Securities and Exchange Commission v. W. J. Howey Co.*, 328 U.S. 293 (1946).

10. Conclusion

Distributed autonomous organizations exist, and are here to stay. Their profit potential is obvious and substantial, particularly because smart contracts and DAOs can reduce transaction costs. However, DAOs are not without risk, and the need to limit liability is necessary for the potential of DAOs to be realized. States are beginning to tailor specialized business entities that address the particular concerns of DAOs, although that does not preclude relevant SEC securities disclosures. While the technology and business models for DAOs are evolving rapidly, the statutory schemes are also going to change, albeit at a slower and delayed pace than the technology. Even so, some companies are taking advantage of particularized corporate forms, and other states will likely follow Vermont's lead in order for those states to remain (or seen to be remaining) competitive.

About the Author

Ronald Chichester is a Texas attorney who is currently Vice President of Technology at JBB Advanced Technologies LLC, a blockchain startup based in Dallas. Ron was originally an engineer in the aerospace industry who, after admission to the Bar, has concentrated on technology-related legal issues. His background made him well suited for handling legal matters related to blockchains, smart contracts, and decentralized autonomous organizations. Ron is also an accomplished software developer who creates tools for automating the legal practice, performing digital forensics, and enabling robots to classify legal opinions for machine learning and artificial intelligence applications.

Tezos and SmartPy: Accessible Smart Contracts on an Upgradeable Platform

By Ronald Chichester

1. Introduction

The definitions of "smart contracts" differ depending upon the orientation of the definer. For example, the Smart Contract Alliance,[1] defines a smart contract as "computer code that, upon the occurrence of a specified condition or conditions, is capable of running automatically according to pre-specified functions. Alternatively, the developer community defines "[a] smart contract, like any contract, establishes the terms of an agreement. But unlike a traditional contract, a smart contract's terms are executed as code running on a blockchain like Ethereum[2]."[3] Similar definitions, but not quite the same.

As with definitions, there are multiple "distributed application" (dApp) blockchains. Besides Ethereum, there is Neo,[4] Tezos,[5] Waves,[6] and several others. "Smart contracts allow developers to build apps that take advantage of blockchain security, reliability, and accessibility while offering sophisticated peer-to-peer functionality — everything from loans and insurance to logistics and gaming."[7] However, because the design of the blockchain itself differs, so too does the behavior of the smart contracts written for those disparate platforms.

---

1 https://digitalchamber.org/initiatives/smart-contracts-alliance/ (last visited on October 29, 2021). The Smart Contract Alliance is an initiative of the Digital Chamber of Commerce, https://digitalchamber.org.

2 Ethereum is the community-run technology powering the cryptocurrency ether (ETH) and thousands of decentralized applications. https://ethereum.org/en/ (last visited on October 28, 2021).

3 *What is a smart contract?*, Coinbase, https://www.coinbase.com/learn/crypto-basics/what-is-a-smart-contract (last visited on October 28, 2021).

4 Neo was founded 2014 and has grown into a first-class smart contract platform. https://neo.org/ (last visited on October 28, 2021).

5 Tezos is another platform for implementing smart contracts and other dApps. However, Tezos was designed to be upgradeable (without forking) and is distributed under an open source license, both of which distinguish it from other dApp paltforms.

6 "Waves is a community-based stack of decentralized open-source technologies to build scalable, user-friendly apps." https://waves.tech/ (last visited on October 28, 2021).

7 *Supra,* note 1.

With that advent of Vermont's blockchain-based limited liability corporations[8], and Wyoming's new corporate form for decentralized autonomous organizations[9], attorneys are encountering clients who want an attorney to opine about the legal effect of the source code for dApps. For those attorneys who have some programming experience, the advent of dApps can be a lucrative addition to a standard business practice. In the recent past, however, programming dApps involved some arcane technologies. Fortunately, newer dApp platforms make the development of dApps easier.

This paper will take one blockchain and associated development environment as a vehicle to discuss (briefly) some of the mechanisms to remedy disputes involving smart contracts. This problem is even more acute because whole corporations are becoming dependent upon blockchains and smart contracts. This paper will take one blockchain and associated development environment as a vehicle to discuss (briefly) some of the mechanisms to remedy disputes involving smart contracts.

2. An Example

Tezos is an open-source and decentralized blockchain network that can perform peer-to-peer transactions and deploy smart contracts. It has a modular architecture and formal upgrade mechanism that allows its network to facilitate formal verification. For those reasons, Tezos has garnered a considerable amount of interest in the dApp developer space.

An organization called Smart Chain Arena has created a Python[10] library called SmartPy[11] that is tailored specifically for developing smart contracts. For anyone even moderately versed in Python, SmartPy is immediately accessible, particularly as compared to the code needed to actually execute on the Tezos platform (see Figure 1).

---

[8] *See,* **11 V.S.A. § 4173 et. seq.,** https://legislature.vermont.gov/statutes/section/11/025/04173 (last visited on October 28, 2021).

[9] *See*, Wyoming Senate Bill SF0038 (2021), https://www.wyoleg.gov/Legislation/2021/SF0038 (last visited on October 28, 2021).

[10] Python is one of the worlds most popular programming languages, and is particularly popular with scientists and engineers. https://www.python.org/ (last visited on October 28, 2021).

[11] SmartPy is available at https://smartpy.io/ (last visited on October 28, 2021).

Figure 1: A comparison of a simple smart contract in Python (left) and Michelson (right)[12]

Development is even easier, because the SmartPy folks have developed an online integrated development environment that you can find at https://smartpy.io/ide.

3. The Dilemma

The Tezos blockchain requires Michelson Contracts (low level) language in order to operate. Consequently, contracts written in SmartPy need to go through a compilation (of sorts) to turn the Python code into Michelson code. Michelson code is arcane and cryptic, which would make it difficult for a jury to follow. Python's syntax, however, is much easier for potential jurors (and everyone else) to grasp. To get to Michelson code, the Python code is first interpreted by a virtual machine called SmartML that is written in OCaml.[13] Then the SmartML code is then compiled to Michelson code that can be executed on the Tezos blockchain. Consequently, the Michelson code is a translation of a translation as shown in Figure 2.

[12] This image is from the SmartPy.io website.

[13] OCaml is a distinct programming language. https://ocaml.org/ (last visited on October 28, 2021).

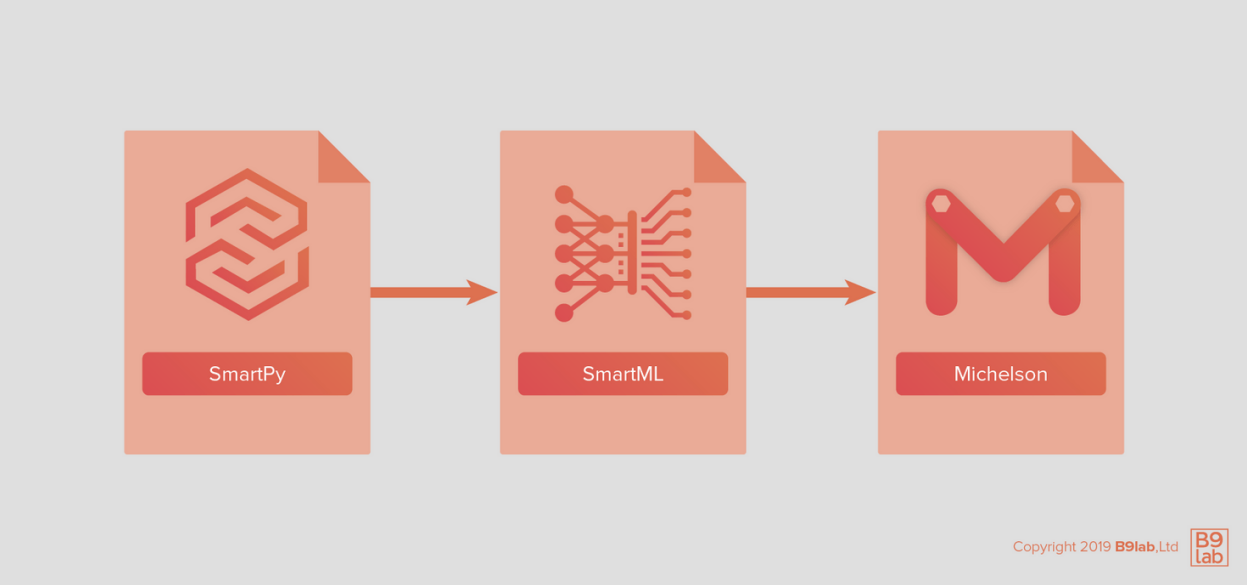


Figure 2. The transition from SmartPy to Michelson code

Whether that double-translation leaves litigators some fodder remains to be seen. Since the Michelson code is what is actually implemented on the blockchain may force the litigator to focus on the Michelson code and ignore the original Python code, which might be a mistake. When considering the Parol Evidence Rule, to which set of code does one turn to discern the mets and bounds of the contract? What the parties intended, or what happened because the parties were ignorant of the (mis-)translation that would ensue? Such questions, however, bely the whole point of a smart contract, namely that the *code* provides the mechanism for arbitrating disputes among the parties.

> "A Smart Contract contains no independent means of enforcement. It is simply executed when a predefined condition, determined by a sensor or a so-called "oracle",[14] either occurs or, within a specified period of time or under some other constraint, does not occur. Many aspects of legal contracts, such as those which rely on the exercise of human judgment and insight, are presently incapable, and may never be capable, of being represented by condition-based functions used in Smart Contracts."[15]

---

[14] Oracles are external servers or processes that retrieve and/or verify external data for blockchains and smart contracts. Since every transaction on the blockchain involves some expense, oracles provide a mechanism for offloading multi-step functionality from the blockchain in order to reduce costs.

[15] Peter L. Michaelson, Esq. and Sandra A. Jeskie, Esq., *Arbitrating Disputes Involving Blockchains, Smart Contracts and Smart Legal Contracts*, SSRN-id3720876 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3720876 (last visited on October 29, 2021).

Okay, so the code is the arbiter of any issues between the contracting parties? Is that it? Michaelson would say that it is.[16] However, opinions differ. Andrew Hinkes suggests that there should be limits to deference to code.[17] Hinkes points out that "… neither legal contracts nor code can prevent a party from filing a lawsuit.[18] Does this leave attorneys having to go through the code at one point or another, and also how to explain this code to a jury? Perhaps not. Amy Schmitz and Colin Rule propose an online dispute resolution mechanism for smart contracts.[19] Amy also suggests that the *blockchain* itself should include a mechanism for online dispute resolution.[20] Tezos doesn't do that, but it is the only blockchain App platform that could be modified to do so. Which begs the question, should some external force (such as a government) mandate that Tezos be modified to include an arbitration mechanism?

The very nature of a public blockchain is that the nodes making up the blockchain do not need (and often do not) lie within a single jurisdiction. Consequently, blockchains such as Tezos tend to be community oriented, and governed in a public manner, which tends to preclude interference by any one jurisdiction. For example, for power consumption reasons (among others), China banned nodes (and thus mining) of Bitcoin within China itself.[21] At that time, China had the *majority* of Bitcoin notes. After China enacted its ban, however, Bitcoin remained in service – without the need for any Chinese nodes.[22] In other words, the distributed nature of

---

[16] *See, ib.*

[17] Andrew Hinkes, *The Limits of Code Deference*, Journal of Corporation Law Vol. 46, Issue 4 (2021) at 869, https://jcl.law.uiowa.edu/sites/jcl.law.uiowa.edu/files/2021-08/Hinkes_Final_Web_0.pdf (last visited on October 29, 2021).

[18] *Id.* at 896.

[19] Amy J. Schmitz and Colin Rule, Online Dispute Resolution for Smart Contracts, 2019 *Journal of Dispute Resolution* 103 (2019). https://scholarship.law.missouri.edu/facpubs/726 (last visited on October 29, 2021).

[20] Amy J. Schmitz, Making Smart Contracts "Smarter" with Arbitration, Alternate Dispute Resolution website, https://go.adr.org/rs/294-SFS-516/images/Making%20Smart%20Contracts%20Smarter%20with%20Arbitration%20by%20Amy%20Schmitz.pdf (last visited on October 29, 2021).

[21] Alun John and Samuel Shen, Tom Wilson, China's top regulators ban crypto trading and mining, sending bitcoin tumbling, Reuters (September 24, 2021), https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/ (last visited on October 29, 2021).

[22] See, e.g., Will Feuer, US passes China as biggest bitcoin mining hub after Beijing ban, New York Post (October 13, 2021), https://nypost.com/2021/10/13/us-passes-china-as-biggest-bitcoin-mining-hub-after-beijing-ban/ (last visited on October 29, 2021).

the blockchain ensured that problems with any one jurisdiction are obviated simply by locating its nodes outside of that particular jurisdiction.

4. Conclusion

Smart contracts are here to stay. There are simply too many aspects about smart contracts that reduce transaction costs for companies.[23] Since the decentralized nature of the blockchain platforms means that they are inherently resistant to pressure imposed by traditional authorities, any kind of arbitration or other resolution mechanisms within a blockchain must come from the developer community.

About the Author

Ronald Chichester is a Texas attorney who is currently Vice President of Technology at JBB Advanced Technologies LLC, a blockchain startup based in Dallas. Ron was originally an engineer in the aerospace industry who, after admission to the Bar, has concentrated on technology-related legal issues. His background made him well suited for handling legal matters related to blockchains, smart contracts, and decentralized autonomous organizations. Ron is also an accomplished software developer who creates tools for automating the legal practice, performing digital forensics, and enabling robots to classify legal opinions for machine learning and artificial intelligence applications.

[23] *See, e.g.,* Mikko Ketokivi and Joseph T. Mahoney, Transaction Cost Economics as a Theory of the Firm, Management, and Governance, https://doi.org/10.1093/acrefore/9780190224851.013.6 (Published online: 26 October 2017, last visited on October 29, 2021).

Digital Zoom

By Antony P. Ng

There is a tendency for people to analogize digital evidence to its analog counterpart. At times those analogies work, but most often they do not. For example, during the recent Kyle Rittenhouse trial, when the prosecution argued that the magnification (pinch zoom) feature of a digital electronic device was the same as using a magnifying glass to produce an enlarged image of an object, the judge intuitively rejected such an analogy.

The usage of a magnifying glass (*i.e.*, a convex lens) to produce an enlarged image of an object can be called *optical zoom*, which is a term borrowed from photography. Optical zoom operates in the analog world—the real world. In fact, human beings generally relate to the real world in an analog manner. For example, the five senses (*i.e.*, sight, touch, smell, taste and hearing) are analog in nature. Thus, analog, without limitation, is the real world.

In contrast, digital is not the real world, but simply a different paradigm created to process information more efficiently. Due to the advancement of modern digital computers, it is much more convenient to process information in a digital form (such as 1s and 0s) than using its analog counterpart. Thus, it is worthwhile to convert information from analog to digital for processing, and then convert the processed information from digital back to analog for human consumption. The conversion details may be different from one case to another, but in general, analog information is initially transposed into digital format to be processed by digital processing machines, and the resultant digital information in the digital world is converted back to analog information in the analog world. This conversion process is similar to the monetary system. If analog is like barter exchange, then digital is like currency. The objects used in barter exchange are real, but bartering is not very convenient for commerce, so the currency system is created to facilitate transactions. Nevertheless, the money in the currency system has to be converted back to actual objects for human consumption.

Digital images (and other digital evidence) fall under the digital world. Enlarging a digital image, such as using the pinch zoom feature, is performed by a technique known as *digital zoom*. Digital zoom is typically done by some form of pixel interpolation in the original digital image via an insertion of new pixels.

Since the resolution of a screen is fixed (or constant), when a portion of a digital image is being zoomed in, the pixels of the digital image will be spread apart from each other on the screen. For example, Fig. 1 shows a letter “C” on a screen with a 5×5 pixel resolution.

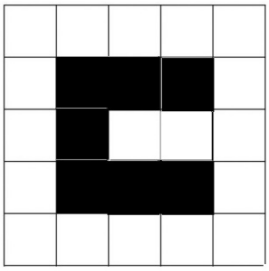


Fig. 1

When the letter "C" is being zoomed in (via a zoom feature such as pinch zoom), the pixels that are adjacent to each other in the original digital image will be spread apart from each other on the 5×5 pixel screen, as shown in Fig. 2. The distance of separation depends on the level of zooming. Suffice to say, the more zooming, the farther apart pixels will be separated from each other. As a result, gaps (white spaces) are created between pixels, and the digital image does not look good with all the gaps among pixels.

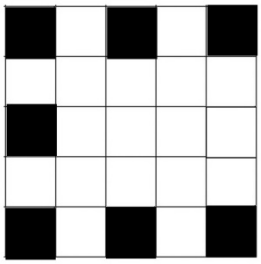


Fig. 2

This is where interpolation comes in. By utilizing the information (such as color) of the adjacent pixels, interpolation employs a mathematical algorithm to calculate and generate some new pixels to fill in the gaps. To continue with the above-mentioned example, the gaps in Fig. 2 can be filled in with new pixels calculated by an interpolation algorithm, as shown in Fig. 3.

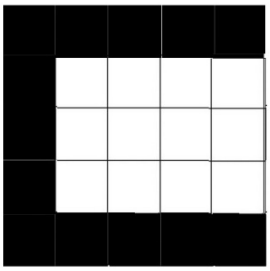


Fig. 3

Interpolation algorithms come in many flavors, such as bilinear interpolation, bicubic interpolation, fractal interpolation, etc. Some interpolation algorithms provide a better result than others (such as a smoother transition instead of a sharp change), depending on the digital image.

With digital zoom, it is clear that the new pixels are generated by an interpolation algorithm, thus, a jury should be made aware of the fact that the new pixels that fill in the gaps are not part of the evidence gathered initially, and that the zoomed-in digital image is not a facsimile of the original.

About the Author

Antony P. Ng is a registered patent attorney practicing in Austin, Texas. Mr. Ng has a bachelor's degree in electrical engineering from Texas A&M University and a master's degree in electrical engineering from Rice University. Mr. Ng also graduated from South Texas College of Law where he served as an assistant editor for the *South Texas Law Review*.

Big Brother–Style Aerial Surveillance Requires a Warrant

By Pierre Grosdidier

The Fourth Circuit Court of Appeals reversed a trial court and enjoined the Baltimore Police Department ("BPD") from proceeding with its pilot Aerial Investigation Research ("AIR") surveillance program.[1] The Court held that because the program enabled authorities "to deduce from the whole of individuals' movements," accessing its data was a Fourth Amendment search that required a warrant.[2]

Under the AIR program, planes flying circles over Baltimore used powerful cameras to capture 32 square miles of the city "per image per second" during daytime, weather allowing. The imagery showed people and cars individually as single pixels. The program did not operate in real-time—even though it had that capability—but allowed its users to build a report of people and vehicle locations and movements before and after each serious crime. The AIR imagery could be integrated with ground surveillance systems such as security cameras, gunshot detectors, and license plate readers. The program intended to retain imagery for 45 days and investigative reports for as long as necessary.[3] Baltimore area grassroots community advocates who frequented crime scenes sued the BPD and its commissioner shortly before the pilot program started.[4]

Plaintiffs Challenged the AIR program under the Fourth Amendment and asked the trial court to enjoin the BPD from proceeding with it. The trial court denied injunctive relief and the Court of Appeals affirmed in a split decision, but then granted an *en banc* rehearing. In the meantime, the pilot AIR program ended, and the BPD deleted all but 14.2% of the captured imagery, which was linked to some 200 past and on-going criminal investigations.

As an initial matter, the Court denied the City's motion to dismiss on mootness grounds.[5] Even though the program had terminated, the BPD retained millions of photographs that tracked movements and could be accessed for the remaining opened investigations. Plaintiffs, who were likely to frequent crime scenes, might appear in the imagery and, therefore, retained a

---

1 *Leaders of a Beautiful Struggle v. Baltimore Police Dept.*, 2 F.4th 330, 333 (4th Cir. 2021) (*en banc*).

2 *Id.*

3 In practice, the AIR program retained most imagery indefinitely. *Id.* at 335–36 n.4.

4 *Id.* at 335.

5 *Id.* at 336.

concrete personal interest in the dispute.[6] This was especially true because the retained imagery was whittled down from the whole on basis of its nexus to crimes.

The Court then focused on the first of the four *Winter* elements that a plaintiff must establish to obtain injunctive relief, namely the likelihood of success of the Fourth Amendment claim on the merits; the other factors being the risk of irreparable harm absent relief, whether the balance of the equities favors relief, and whether relief is in the public's interest.[7]

The Fourth Amendment historically protected against unreasonable—and unwarranted—searches and seizures of homes and personal effects.[8] In its landmark 1967 *Katz v. United States* decision, in response to technology's encroachment into private lives, the U.S. Supreme Court extended the Fourth Amendment's aegis to situations where a person has a subjective expectation of privacy that society is willing to recognize as reasonable.[9] Under *Katz*, the Court held that the police needed a warrant to record the private conversation of a person in a phone booth. Applying *Katz*, the U.S. Supreme Court's recently held in *Carpenter v. United States* that obtaining cell-site location information ("CSLI") required a warrant because its ability to reconstruct a person's past movement through his or her phone signals invaded the person's reasonable expectation of privacy.[10]

The Fourth Circuit held that "*Carpenter* applies squarely to this case" because "the AIR program 'tracks every movement' of every person outside in Baltimore."[11] Even factoring the nighttime and weather-occasioned interruptions, this surveillance can record a person's repeated movements from place to place, from which one may deduce more about the person's personal life than one ever could by observing individual trips. These deductions, the Court added, "go to the privacies of life, the epitome of information expected to be beyond the warrantless reach of the government."[12] Moreover, these intrusions into a person's "associations and activities" infringe on the reasonable expectation of privacy that the person has in the whole of his or her movements.[13] The court held that because the AIR program tracked people much as CSLI does, accessing its data was a search and the program's warrantless operation violated the Fourth

---

6 *Id.* at 337.
7 *Id.* at 339; *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7 (2008).
8 *Id.* at 339–40.
9 *Id.* at 340; *see Katz v. United States*, 389 U.S. 347 (1967).
10 *Id.* at 341 (citing *Carpenter v. United States*, --- U.S. ---, 138 S. Ct. 2206, 2213–23 (2018)).
11 *Id.*
12 *Id.* at 342.
13 *Id.* at 342, 346.

Amendment.[14] For this reason, the Court concluded, Plaintiffs' Fourth Amendment claim was likely to succeed on the merits.

The Court also briefly reviewed the other three *Winter* factors, which it held supported preliminary relief. The likely constitutional violation satisfied the irreparable harm factor as a matter of law, the enjoinment of a potential constitutional violation did not harm the state, and the "public interest favor[ed] protecting constitutional rights."[15] In conclusion, the Court held that the district court abused its discretion in denying Plaintiffs' motion for a preliminary injunction and it reversed and remanded.

About the Author

Pierre Grosdidier is an attorney in Houston. 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), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Chair-elect for 2021-22.

[14] *Id.* at 346.

[15] *Id.* (citations omitted).

A Body-Worn Camera Does Not Dispense the Need for a Warrant

By: Pierre Grosdidier

The use of body-worn cameras by police officers during interactions with the public presumably has the merit of keeping everybody honest, but the recordings come with strings attached, as the recent Massachusetts case *Commonwealth v. Yusuf* illustrates.[1] In *Yusuf*, the Boston police intervened in a domestic disturbance that involved the defendant, his sister, and his girlfriend.[2] A police officer's body-worn camera recorded his field of view during his coming and goings in the home including, at one point, "floral-printed curtains" adorning a bedroom window. The officer later uploaded the video recording in a police database, and a detective used the video to secure a search warrant in an unrelated investigation that led to the defendant's conviction on firearms offences. The Massachusetts Supreme Judicial Court held that the use of the body-worn camera during the disturbance was not a search under the Fourth Amendment, but that the later use of the recording for an unrelated investigation was—and required a warrant.

The defendant had been the target of an investigation for firearms offenses completely unrelated to the domestic disturbance, and a detective had been searching for a basis to secure a search warrant for his home.[3] Sometime after the disturbance, the defendant posted a video of himself holding a firearm in a room with matching "floral-printed curtains visible in the background." The detective secured a search warrant based on the matching curtains and the search resulted in the seizure of narcotics, a firearm, ammunition, and marijuana.

During his bench trial, the defendant moved to suppress, *inter alia*, the body-worn camera video recording and the fruits of the search. The trial judge denied the motion and found the defendant guilty of unlawful possession of a firearm and ammunition.[4] On direct appeal to Massachusetts highest appeal court, the defendant argued that both the warrant-less use of a body-worn camera inside the home and the use of the recording in the unrelated firearms investigation violated the Fourth Amendment's prohibition against unreasonable searches.

---

1 173 N.E.3d 378 (Mass. 2021).

2 *Id*. at 381.

3 *Id*. at 383.

4 *Id*. at 384-85.

As the court noted, the home is expressly protected by the U.S. Constitution's Fourth Amendment and the Massachusetts Constitution's Article 14.[5] Given the home's sanctity, it is entirely "safe from prying government eyes."[6] Be that as it may, the court rejected the defendant's claim that the officer's use of a body-worn camera in his home amounted to a constitutional search. The officer was lawfully in the home at the invitation of the defendant's sister and in response to her request for assistance in the domestic disturbance. The record showed that the officer had not ventured in the home beyond the locations where he was required to perform his duties. The video captured only the plain view observations in which the defendant had a diminished expectations of privacy because of the officer's lawful presence in the home. In effect, the body-worn video was not substantially different from crime scene pictures that police officers routinely take without violating constitutional rights. A violation would have occurred had the officer ventured beyond the locations necessary to deal with the disturbance, but such was not the case here.[7]

The subsequent use of the video in the firearms investigation was another matter, however. As other courts, including the United States Supreme Court, have already stressed, improvements in the power of technology and their adoption by authorities do not shrink privacy rights.[8] In this case, the court called the ability of police officers to review the video of the defendant's home interior at any time after the disturbance and for wholly unrelated reasons "the virtual equivalent" of the reviled "general warrants" and "writs of assistance" of the colonial era. Moreover, the later review of the video for reasons unrelated to the domestic disturbance defeated the rationale for making the recording in the first place, which was to create a record of the interaction and protect its participants from misconduct or false accusations. Giving access to the video for another unrelated reasons was the equivalent of allowing detectives "to peer into the defendant's home for evidence to support an unrelated criminal investigation" without a warrant.[9] The court held that such conduct was worthy of Orwellian Big Brother and amounted to a presumptively unreasonable warrantless search.

---

5 *Id*. at 386.

6 *Id*. (internal quotations omitted).

7 *Id*. at 386-390 ("Plain view observation cannot be used as a pretext for a general exploratory search of the home.").

8 *Id*. at 392.

9 *Id*. at 393.

About the Author

Pierre Grosdidier is an attorney in Houston. 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), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Chair-elect for 2021-22.

Five Things You Can Learn About Cybersecurity from the Recent Presidential Order

By Michael Curran

In May 2021, the President of the United States signed the ***Executive Order on Improving the Nation's Cybersecurity*** (referred to in this article as the "National Cybersecurity Order"). If you followed the news last year, you know that cyberattacks on the nation's infrastructure are escalating. You won't be surprised to know that cyberattacks on businesses, law firms and individuals are increasing as well.

The National Cybersecurity Order contains recommendations for what the government needs to do to improve its defense against growing cyberthreats. As lawyers trying to protect our firms and our clients from data breaches, fraud and identity theft, what we can we learn? Let's look at a few highlights that can be applied to protect your firm and your clients. First, here is a little background.

The Order starts by stating: "The United States faces persistent and increasingly sophisticated malicious cyber campaigns." No one can argue with that. We are all facing persistent and increasingly sophisticated cyberattacks and scams. How many email scams and robocalls do you and your clients receive every month?

Next, the Order says the government must "improve its efforts to identify, deter, protect against, detect, and respond to" the actions of these cybercriminals. These are great goals for the government, and most of these goals will apply to lawyers and their clients as well. Here are five (5) things you can do based on the government recommendations to help stop cybercrimes.

1. Remove Barriers to Sharing Information

The first substantive section of the National Cybersecurity Order discusses breaking through some of the red-tape that different government agencies face related to sharing threat information. We all face barriers to sharing threat information. For lawyers, protecting confidential client data is so engrained into the job that sharing information of any kind can be difficult. Two common barriers that everyone faces related to sharing cyber-fraud details are:

1. Embarrassment about being a victim of fraud, and
2. Uncertainty regarding how to report cybercrimes.

Law firms and their clients need to overcome their embarrassment and fear if they become a victim of a cybercrime. According to Statista, over 37% of Internet users in the United States have been a victim of bank card or online banking fraud. More than one out of three is a big percentage. If you, your firm, or your clients are a victim, then you are not alone.

We also all need to know how to report cybercrimes. Criminals want to steal information and ultimately money, and they want to get away with it. There are plenty of regulations that require businesses of all types to report breaches, and a failure to report can result in serious fines and penalties. If individuals don't report a cybercrime, then the criminals win will. The government Website that helps individuals report cybercrimes and scams can be found here: https://www.usa.gov/stop-scams-frauds. Another good step for individuals is telling a trusted contact about the cybercrime to get help if needed.

2. Modernize Approach to Cybersecurity

Next, the National Cybersecurity Order states that the government must adopt modern security best practices. Change is hard, and many people have probably been following the same habits related to personal cybersecurity for the past 5 years. It is likely time that you should adopt some new best practices to protect yourself, your firm, and your clients from cybercrimes.

When was the last time you changed your passwords? Do you use multi-factor authentication? Do you always use a VPN when using public networks? Has your firm taken advantage of any free training options related to phishing? There are many ways to improve protection against data breaches for law firms and their clients, and often the simplest data protection measures can have the most significant impact.

3. Enhance Software Security

The National Cybersecurity Order discusses how the security of the software that the government uses is vital. We rely on software to perform more of our daily routines today than we did a few years ago. Therefore, we need to make sure that we use software from reliable vendors. Terms and conditions of software companies are notoriously long and difficult to understand, but you and your clients still need to realize what you are risking by using the latest app or social media tool.

What if your information was being sold to partners of the free app or social media company? Sadly, it probably is. As the saying goes, if you are not paying for software, then you are not

the customer. You are the product, and your information is being sold to others. Make an effort to understand how a software company makes money and uses your information. Also, lawyers and individual clients should think twice before posting detailed personal information that can be used by cybercriminals.

4. Establish a Cyber Safety Review Board

The government is directed to form a board that will review threats and make recommendations. Maybe it is difficult for all law firms to form a review board of experts. But, we can still learn from the experts. Make it a habit to read one new article or book per month that can help you improve cyber safety for your firm and your clients. To get you started, here is an article by PC Magazine: https://www.pcmag.com/how-to/12-simple-things-you-can-do-to-be-more-secure-online. Every little bit of knowledge may improve your chances of avoiding a data breach.

5. Standardize Playbook for Responding to Cybersecurity Threats

The National Cybersecurity Order also recognized that there was a lot of inconsistency regarding how parts of the government identified and recovered from cybersecurity vulnerabilities and incidents. Law firms and clients can be inconsistent as well, and not everyone has a playbook for responding to threats. What could you do to create a standard playbook for how you will reduce vulnerabilities and recover from cybercrime incidents? To get started, here are a few ideas of what to include in a cybersecurity threat playbook.

- Make a backup of important documents and data and keep them safe
- Investigate any suspicious activity
- Determine if there have been any losses
- Report incidents to authorities and notify anyone else who may be at risk as required
- Keep documents and write down details regarding the incident
- Investigate procedures for restoring any lost data
- Change passwords on vulnerable accounts
- Write down lessons learned to minimize future risks

The National Cybersecurity Order is a reminder of the threats that we all face from cybercrimes and fraud. It outlines several steps the government is taking to reduce risk, and there is a lot that law firms and their clients can learn from these national cybersecurity recommendations. For more information regarding improving your cybersecurity, there are many articles available in *Circuits* by the Computer & Technology Section of the State Bar of Texas.

About the Author

Michael Curran is a Texas attorney and legal tech entrepreneur focused on using technology to address today's largest legal and social issues. Michael is a Past Chair of the State Bar of Texas Computer and Technology Section, and a regular legal technology speaker. Michael received his law degree from South Texas College of Law and his MBA and BBA from the University of Texas at Austin.

Michael is co-founder of Guide Change, a startup business that financial professionals use to help their clients build Social Wealth. Guide Change technology offers advice to address many of the non-monetary issues associated with successful aging such as caregiving, aging in place, and avoiding financial exploitation. During his career, Michael has held positions as an in-house counsel, corporate executive, eDiscovery consultant, and litigation attorney.

U.S. Supreme Court Narrowly Construes the TCPA's Autodialer Definition

By Pierre Grosdidier

Among its several consumer-friendly provisions, the Telephone Consumer Protection Act ("TCPA") of 1991 protects consumers from robocalls, which originate from "automatic telephone dialing systems," or autodialers. 47 U.S.C. 227(a)(1). The statute defines an autodialer as

> (1) . . . equipment which has the capacity—
>
> (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and
>
> (B) to dial such numbers.[1]

The issue in *Facebook, Inc. v. Duguid* was whether the modifying clause "using a random or sequential number generator" applied to equipment that "stored or produced telephone numbers," or only to those that produced them.[2] The latter "broad" statutory construction implied that any equipment that merely stored and dialed numbers qualified as an autodialer—a construction that encompassed all hand-held devices that store and dial phone numbers.[3] Circuit Courts were split.[4] In a very textual decision, U.S. Supreme Court opted for the narrow statutory construction.[5]

Duguid, the plaintiff-appellee, sued Facebook after it sent him several text messages that alerted him that someone had attempted to access his Facebook account. Duguid had no such account, and the phone number must have been associated with another Facebook account owner before the number was reassigned to Duguid.[6] Be that as it may, Facebook stored the

---

1 *Id.*

2 --- U.S. ---, 141 S. Ct. 1163, 68-69 (2021).

3 *Id.* at 1171 (citing W. Eskridge, *Interpreting Law: A Primer on How To Read Statutes and the Constitution* 67-68 (2016)).

4 Compare *Duguid v. Facebook, Inc.*, 926 F.3d 1146 (9th Cir. 2019); *Duran v. La Boom Disco, Inc.*, 955 F.3d 279 (2d Cir. 2020); and *Allan v. Pennsylvania Higher Educ. Assistance Agency*, 968 F.3d 567 (6th Cir. 2020), with *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458 (7th Cir. 2020) (Barrett, J., for the court); *Glasser v. Hilton Grand Vacations Co.*, 948 F.3d 1301 (11th Cir. 2020); and *Dominguez v. Yahoo, Inc.*, 894 F.3d 116 (3d Cir. 2018).

5 *Id.* at 1167.

6 *Id.* at 1168 n.3.

number but did not generate it randomly or sequentially. Duguid sued Facebook, alleging a violation of the TCPA.

The Court applied the "series-qualifier canon," which holds that "'[w]hen there is a straightforward, parallel construction that involves all nouns or verbs in a series,'" a modifier at the end of the list "'normally applies to the entire series.'"[7] The Court held that qualifying both antecedent verbs "store" and "produce" with the modifying sentence "produce[d] the most natural construction." This conclusion was reinforced by the "concise" and "integrated" clause "store or produce telephone numbers to be called," which "hangs together as a unified whole." Finally, this construction "heed[s] the commands of its punctuation" given the location of the comma that precedes the modifying clause.[8] This comma "'is evidence that the qualifier is supposed to apply to all the antecedents instead of only to the immediately preceding one.'"[9]

The Court rejected plaintiff-appellee Duguid's argument that it should apply the "rule of last antecedent," whereby the modifying clause applied only to the noun or phrase that immediately precedes it. The Court noted that it had refused to apply this rule to an integrated list, as here. Moreover, the last antecedent in this case was "the telephone numbers to be called," not the verb "produce."[10]

In conclusion, the U.S. Supreme Court held that under the TCPA's definition, an autodialer must use a random or sequential number generator to either store or produce telephone numbers. Equipment that merely stores numbers, like Facebook's login alert system, does not qualify.[11]

---

7 *Id*. at 1169 (citing A. Scalia & B. Garner, *Reading Law: The Interpretation of Legal Texts* 147 (2012) (Scalia & Garner) (quotation modified)).

8 *Id*. at 1169-70.

9 *Id*. at 1170.

10 *Id*.

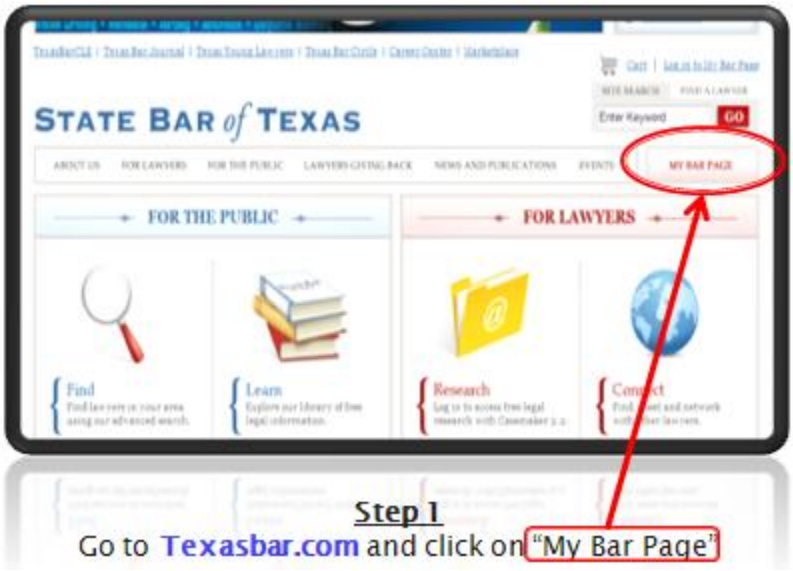
11 *Id*.

About the Author

Pierre Grosdidier is an attorney in Houston. 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), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Chair-elect for 2021-22.

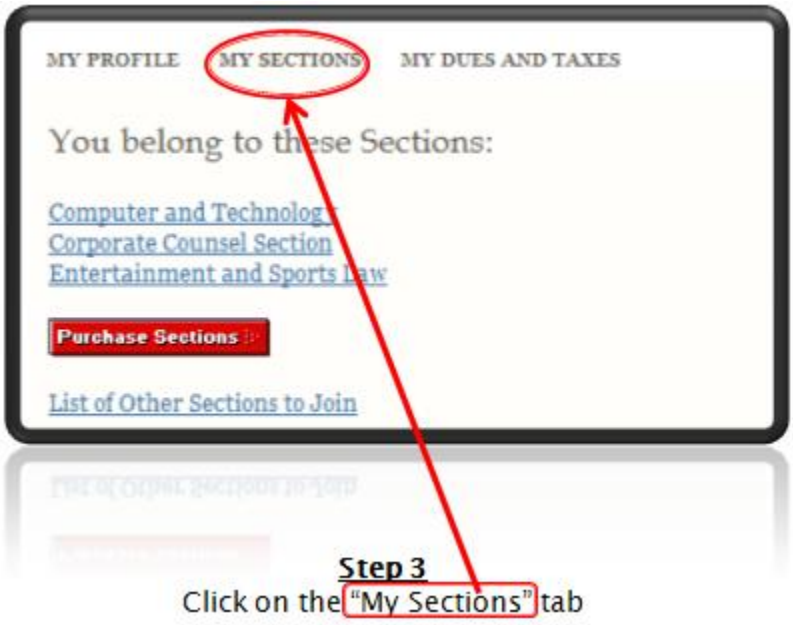
How to Join the State Bar of Texas Computer & Technology Section

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"

Step 2
Login using your bar number and password
(this will be the same information you'll use to login to the Section website)



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:
Elizabeth C. Rogers – Austin – Chair
Shawn Tuma – Plano – Immediate Past Chair
Pierre Grosdidier – Houston – Chair Elect
Reginal Hirsch – Houston – Treasurer
William Smith –Austin – Secretary

Circuits Editors:
Matthew Murrell – Austin

Webmasters:
Ron Chichester – Houston
Rick Robertson – Dallas

Appointed Judicial Members:
Judge Xavier Rodriguez – San Antonio
Hon. Roy Ferguson – Alpine

Term Expiring 2024:
Justin Freeman – Austin
Zachary Herbert – Dallas
Grecia Martinez – Dallas
Guillermo "Will" Trevino – Austin

Term Expiring 2023:
Craig Haston – Houston
Matthew Murrell – Austin
Christine Payne – Austin
Mitch Zoll – Austin

Term Expiring 2022:
Lavonne Burke Hopkins – Houston
Michelle Mellon-Werch – Austin
Gwendolyn Seale – Austin
Alex Shahrestani – Austin

Chairs of the Computer & Technology Section

2021–2022: Elizabeth C. Rogers
2020–2021: Shawn Tuma
2019–2020: John Browning
2018–2019: Sammy Ford IV
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