FOLEY

FOLEY & LARDNER LLP

Silicon Valley Business, Legal and Technology Developments in Review

2021

FOLEY.COM

TABLE OF CONTENTS

Seven key emerging technologies to drive economic outcomes in 2022: Adaptation of law and policy and capital deployment will determine the winners

Foley & Lardner LLP attorney Louis Lehot discusses seven key emerging technologies that are drawing global venture funding.

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on Westlaw Today on November 1, 2021

As the end of the record year 2021 approaches, global venture investors are racing to deploy capital at an unprecedented pace. Global venture funding more than doubled in the third quarter of 2021 compared to the year-ago period, with seven key emerging technologies garnering the most strategic attention.

As we parse the data across geographies, we see the development of a decoupled and bipolar investing market divided between the United States and China, with Asia growing fastest.

The two superpowers of venture are competing in seven key emerging technology areas to drive more rapid economic growth and ultimately the security of their respective nations. America's ability to compete for the best entrepreneurs and engineers, the most capital, and the highest level of market access will determine whether America remains a leading superpower.

America's failure to compete in these key emerging technologies could cause it to be eclipsed by China. Both national security and economic returns hang in the balance.

While a great debate rages as to whether America is in decline, it continued to garner nearly 50% more investment from venture capital investors than all of Asia combined. But among the top ten global investors, three hail from China, and another from Japan (but whose largest asset continues to operate primarily in the People's Republic).

For 2022 and the remainder of this decade, whether it's competition for capital, market access, or talent, investors and governments alike will be focused on artificial intelligence and automation, quantum computing and the semiconductor industry, networking (whether in the cloud, on the edge or in the fog), >5G wireless bandwidth speeds, Blockchain and other distributed ledger technologies, and ultimately, biotechnologies like CRISPR, that will help us live longer and fight disease.

Today's legal systems, laws, and policies evolved out of centuries' old philosophies and cultures. While yesterday's answers to age-old questions may continue to be relevant, new approaches that modernize legal systems to stimulate the development of these technologies could be as important as the deployment of capital in determining the winners of the new technology race.

Artificial intelligence and automation

Artificial intelligence plays a significant part in almost every industrial sector and offers tremendous benefits to industries and individuals. Many companies have adopted automation to increase their efficiency and gain a competitive advantage.

AI-powered wearable devices help provide tailored treatments, and self-driving vehicles are another phenomenal achievement of AI.

AI enables automation, and automation means productivity. Financial and strategic investors are hungry for more. In the future, we can see AI combined with other technologies and companies widely adopting AI1 for their business operations.

Quantum computing and semiconductors

Quantum computers use quantum-mechanical phenomena to perform computation at much faster speeds than classical computers. Through the use of superposition and entanglement, quantum computers are the next generation of supercomputers.

Quantum computers can process equations that last generation supercomputers would take thousands of years to perform. The massive capabilities of quantum computers can also decrypt encrypted data easily. As practical quantum computers edge closer to reality, others are developing algorithms that are intractable even for quantum computers.

Our current legal system has not contemplated the world of probabilities that quantum computing will enable. Cybersecurity will be endangered, and unhackable quantum cryptography will need to be created in response. Safety systems to deter and prevent cybercrime is urgent. The terabytes of personal information will need to be protected and collected at each point of transmission, wherever it is stored, analyzed, monetized, and used.

Competition will need to be preserved while rolled out, lest the first adopter squelches all others. Cloud compute power and orchestration platforms will need to evolve. Ultimately, we will have to decide what decisions are appropriately made by a quantum computer versus a human.

Meanwhile, the United States government will seek to protect its position in the design and fabrication of semiconductors. In contrast, China aims to decouple its dependence on U.S. semiconductor manufacturers with home-grown alternatives.

Networked compute power in the cloud, on edge and in the fog

Global business is now interlocked by overlapping computing networks that migrate from the edge of your device to the cloud and back again. Increasingly, data lives in some foggy place between the edge and the cloud, which can map the shortest distance between the two, optimizing both bandwidth and compute power.

Cloud services offer significant cost savings compared to local on-premises solutions. Maintaining a local or on-premises database requires sophisticated equipment, real estate, and experienced personnel to manage and maintain it.

With cloud service, the data becomes more flexible as it can be accessed from anywhere. Alternatively, some data is most productive when it lives on the edge of the device, where it is collected, analyzed, and monetized closest to its point of use.

The migration to automated cloud computing power and back to the closest edge of the network has only accelerated. Containers are increasingly deployed across the public, private, and hybrid cloud ecosystems to enable the transfer, storage, analysis, and response layers.

Cloud orchestration platforms like Kubernetes and Docker have emerged as ubiquitous technologies to build, deploy and manage containerized applications using automation, and investors have noticed.

Cloud orchestration platforms like Kubernetes and Docker will see more interest from investors since containers and virtualization technologies make a company's applications and other assets more portable to other cloud services, not locking them into one provider and allowing an enterprise to choose between hybrid and hybrid public cloud options.

Legal systems need to evolve to account for the location of the servers, how and where the clusters of containers travel, and how to protect the data. Jingoistic legislators in each of Europe, the United States, and China are competing to be the most stringent in safeguarding personal information. Inevitably, they will need to best balance the monetization of data that lives or travels through their clouds and networks against the right to personal privacy.

5G

5G, the next generation of cellular bandwidth connectivity, has already started in some parts of the world, providing greater connectivity speeds. One of the most vital characteristics of 5G is Massive Input Massive Output (MIMO). 5G can transmit and receive data from a wide variety of sources, and with 5G, transmission and reception of data can happen on the same wavelength at the same time.

China, the United States, and Europe have engaged in a high stakes battle for hegemony in the 5G market, with China coming strong out of the gate.

While the war for dominance in 5G deployment rages on, the future of the next generation of bandwidth hangs in the balance.

Meanwhile, legal questions abound regarding who gets access, when and where, who pays for it, where the data goes, who protects the privacy of transmitted data, and ultimately, the balance between liberty and authoritarianism.

Blockchain

Blockchain is a specific kind of database, with the difference between a typical database and blockchain being how the data will be stored. In a standard database, the data is categorized into well-defined rows and columns and stored. While in a blockchain, the data are stored in blocks, and each block is connected to its predecessor and successor, forming a chain-like pattern. Hence the name "blockchain."

The data in the blockchain are encrypted. They are stored in a hash format, with all of the blocks in the blockchain networks interconnected. It's virtually impossible to decrypt the data in a blockchain network without the right keys, making blockchain effective against cyberattacks and data leakages.

Lately, huge financial corporations and multi-national corporations have started adopting blockchain technology. In the upcoming years, the genuinely decentralized characteristics of blockchain will create an abundance of opportunities across multiple industries, such as the healthcare industry, which is often subjected to cyberattacks as it contains much sensitive information.

Adopting blockchain technology to store records could prevent any cyberattacks in the healthcare industry. The total revenue spent globally on blockchain solutions is expected to be 6.6 billion by 2024.[2]

Biotechnology and genetic engineering

CRISPR, Clustered Regulatory Interspaced Short Palindromic Repeats technology, is a significant breakthrough in genetic engineering, allowing for altered DNA sequences and modifying gene function. This technology will bring about significant advancements in medical sciences and could potentially cure diseases with its capabilities to change the DNA structure.

Through the end of the third quarter of 2021, funding for healthcare ventures globally had exceeded every prior whole year by more than 25%, with America way ahead of the pack. Despite the projected growth and abundant investment capital, there are dangers that legal and ethical concerns related to genetic research could restrain the growth of gene-editing technologies. There's the possibility of off-target effects and other ethical problems that could cause government regulators to put a hold on development.

Regulations must keep pace with the change that CRISPR-Cas9 brings worldwide to research labs. Developing international guidelines could be a step towards establishing cohesive national frameworks. Ethical questions relating to biotechnology will arise with each innovation.

Tensions between the best interests of an individual patient and society at large will only get more pronounced. The response to the pandemic and vaccination mandates is only but one example.

Conclusion

The technology field never stops developing, and these technologies will play an increasingly important role in our lives. In all of these key emerging technology areas, America and China compete to demonstrate that their system drives a better way of living, working, and relating to one another.

At issue in the new technology race is whether a democratic system where individual liberties and private property are paramount can prevail over a centrally governed command system where the interests of society prevail over the individual.

Notes

[1] https://bit.ly/2ZHpFq1

[2] https://bit.ly/3vViSoD

Navigating the legal cloud: How to manage data and intellectual property with Cloud Orchestration Platforms

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on IP Watchdog on October 13, 2021

"As the virtual world explodes with data, 'containers' are the paradigm by which they are growing."

As the way we live and work has increasingly moved into virtual environments (I like to call it a legal metaverse), the boundaries between physical, digital, and biological worlds become blurrier by the day. Sensors lie within devices installed across every aspect of our home, office and mobile environments, connected from the edge of each of your devices to networks that are both local and cloud-based (with many in a foggy place between the two). The ensuing data traffic requires massive computing power for transfer, storage, analysis, and response. The migration to automated cloud computing power has further accelerated the deployment of containers across the public, private and hybrid cloud ecosystems for the transfer, storage, analysis, and response layers. Kubernetes and Docker have emerged as ubiquitous technologies to build, deploy and manage containerized applications using automation, and investors have noticed. Understanding the key legal issues will enable more successful client relationships for both vendors and customers, and inevitably growth and value creation.

What is a Container?

A container is an executable unit of software that packages application code with the ancillary components needed to deploy in public, private, and hybrid clouds, enabling it to run on any IT infrastructure. We call it a "container" because it stands alone, away from the host operating systems. It has revolutionized how businesses build and scale their applications.

Kubernetes

Kubernetes, developed and designed by engineers at Google, is an open-source container orchestration platform that automates many manual processes involved in managing and scaling containerized applications. One of the significant advantages of using Kubernetes is that it gives you the platform to schedule, manage and run containers on clusters of physical or virtual machines, also known as VMs.

Docker

Docker is an open source containerization platform that helps developers build, deploy and manage containers. While it is an open source project initially created in France, it moved to the United States and was acquired by Mirantis in 2019. It is backed by a vibrant developer community that shares containers across the Internet via a Docker Hub. Docker accomplishes orchestration tasks with its tool called Docker Swarm. While distinct technologies, Kubernetes and Docker are complementary and can work together to deliver computing power.

As the virtual world explodes with data, containers are the paradigm by which they are growing, and Kubernetes and Docker are the tools by which they are built, managed, deployed, and optimized.

Dealmakers Looking to Enable the Hybrid Cloud

The space has become an attractive and robust ground for investments and dealmaking. By way of example, according to CrunchBase News, San Jose, California-based Lacework, with a cloud security platform including securing workloads in Kubernetes, closed a $525 million round led by Sutter Hill Ventures and Altimeter Capital that values the company at more than $1 billion. IBM's Red Hat acquired Mountain View, California-based StackRox, a Kubernetes-native security platform. Previously, the enterprise business of Docker was acquired by Mirantis.

Legal Relationships in a Container

For businesses that operate with data, managing the adjacent legal relationships will be essential. Is your vendor providing you with Software-as-a-Service product that will enable you to within your clusters of containers? Or is it a professional services firm moving clients to one or another cluster or orchestration platform? Or are they writing code to manage Kubernetes? What are the standards of quality that will be met? Who owns the code? Is there a license-back to re-use that same code or derivative code for other customer engagements? Or are you the vendor?

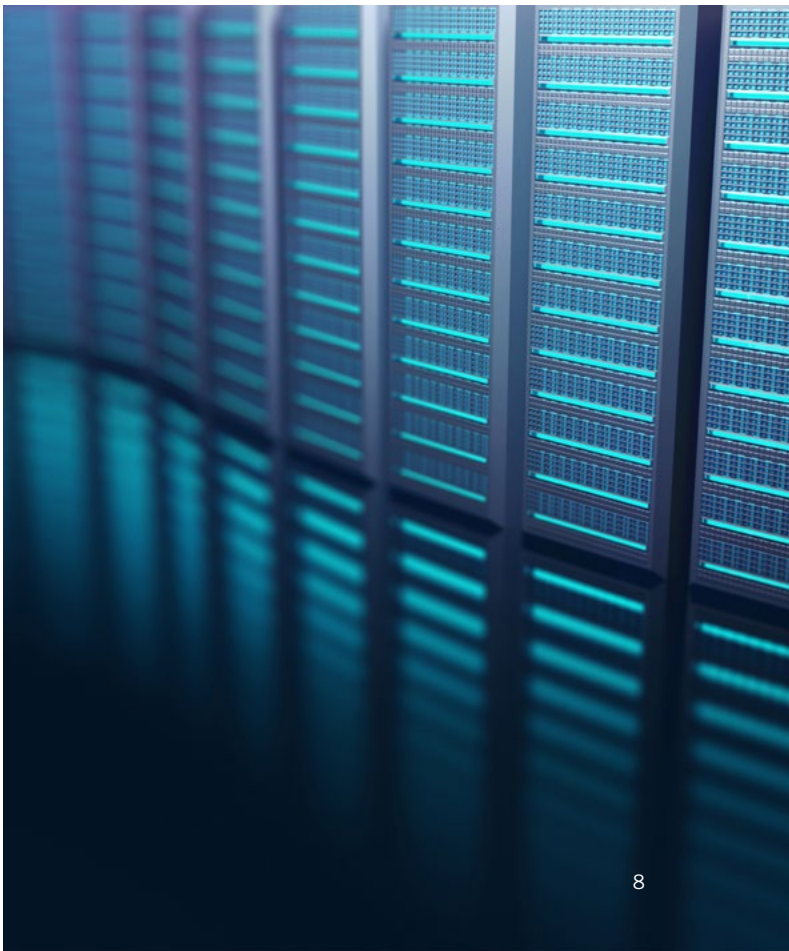
If you are a vendor and offer the intellectual property to clients, whether in software or code, you need to own it, license it, and have the right to sub-license it. If you are a software company, this starts by making sure that every employee or consultant signs an invention assignment agreement.

Whether you are the customer or you are the vendor operating with clusters, the data in the container must be protected and handled pursuant to applicable legal norms. While we used to worry only about the European Union's **General Data Protection Regulation** (GDPR), there are even more intrusive regulations with teeth coming out of California, and even China. Compliance with data protection regulations is subject to audit, and in any investment or M&A process, a deep diligence dive. Failure to protect data will cause an investor or a buyer to disconnect from your zoom.

Welcome to the Future…in a Container

Kubernetes and Docker should continue to see interest from venture capital as well as strategic investors, since containers and virtualization technologies make a company's applications and other assets more portable to other cloud services, not locking them into one provider and allowing an enterprise to choose between hybrid and hybrid public cloud options.

New technologies that monitor and understand what the data is saying are on the horizon. The next wave of cloud-orchestration platforms is here. Making sure that legal relationships are well defined will enable your company to benefit, thereby increasing both your business and your value.



The IPO Markets are changing, and so is the lock-up agreement

Authors: **Louis Lehot | llehot.foley.com, Eric Chow | echow@foley.com**

This article was originally published on Foley.com on March 30, 2021

An initial public offering (IPO) is a crucial time in the life of a company and its stakeholders. Initial investors, employees, and executives can profit from the public listing, and the company can raise additional capital. But IPOs come with a number of limitations, some required and some just common. Today, lock-up agreements, once a common feature of IPOs, face a changing and uncertain future.

What is a lock-up agreement?

A lock-up agreement is a set period of time during which company insiders are restricted from selling shares, subject to limited and highly negotiated exceptions. As the SEC notes, this lock-up period usually lasts for 180 days, and while federal laws require companies to disclose these agreements, lock-ups are not mandated except in certain states with "blue sky laws."

Lock-up agreements exist to help minimize fluctuations in a company's share price when the stock first hits the public market. By preventing insiders from dumping shares quickly, a lock-up agreement restricts the supply of stock for sale on the public market, which, in turn, reduces the risks of potentially causing the stock price to plummet at an especially critical time. In addition, a company typically agrees not to issue additional securities. The lock-up agreement is usually heavily negotiated with the underwriter. As Crunchbase notes, once a lock-up period ends, the free-market sale of stock shares by insiders can serve as a barometer of sorts. If insiders hold their shares, perhaps they believe the price will rise, but selling shares may suggest otherwise.

With all the changes in market dynamics, investor priorities, and consumer interests due to the pandemic, the outlook for 2021 may be difficult to discern, but we can follow some trends. From our experience, the 180-day lock-up period is still, by far, the most common length. But despite that consistency, in recent times, there is a trend for companies to structure lock-ups with different lock-up periods for different parties.

Lock-up agreements in de-SPAC transactions

SPACs, or special-purpose acquisition companies, are also gaining traction as an alternative to IPOs to get private companies to market faster and at a lower price point. In a SPAC transaction, a newly formed company raises funds in the public markets via IPO, and then uses the proceeds to acquire a private operating company. Lock-up periods for SPAC transactions are typically longer than traditional IPOs (e.g., one year or more).

No lock-up agreements in direct listings

On the other hand, some companies are opting to achieve public listing by way of direct listings, as opposed to IPOs. In direct listings, existing shares are made available for trading in a public market without an underwritten offering, and, thus, without restrictions imposed by standard lock-up agreements, giving its existing shareholders immediate liquidity. Although underwriters are not engaged and these companies can save on costs, the companies' ability to raise new capital is more restricted compared to IPOs. Spotify, Slack, Asana, and other well branded e-commerce businesses have successfully gone public via direct listing. Companies with track records of strong growth and healthy financials are good candidates for direct listings and can go public with no lock-up agreements.

What to expect

To a certain extent, the deviations from the standard 180-day period of the lock-up arrangements should not be surprising. We have seen similar trends of increasing democratization and disintermediation, particularly in the technology industry. Time will tell whether lock-up agreements will be less important in listing processes going forward, or even end entirely.

A checklist of legal considerations for the NFT marketplace

Authors: **Louis Lehot | llehot.foley.com, Catherine Zhu | czhu@foley.com**

This article was originally published on Crunchbase News on November 9, 2021

With the growing interest from consumers and asset managers, investors as well as entrepreneurs interested in digital assets, we have created this checklist for monetizing items with unique artistic content characteristics through nonfungible tokens (NFTs).

We have seen businesses that aggregate content to be monetized on an NFT, while others mint the tokens or build NFT marketplaces, and many more that intermediate payment transactions between the creators, the licensors, the marketplaces, and the buyers, the sellers and the exchanges upon which they trade.

Each of these types of businesses, and the transactions in which they participate, will need to consider the legal ramifications of still-developing law, policy and regulation applicable to each link in the chain of =NFT commerce.

But first, a quick primer: An NFT marketplace is a platform that connects content creators with NFT buyers with NFT sellers. Sellers mint NFT tokens with the created digital asset in this platform, and buyers can browse listed assets and buy or participate in an NFT auction. There are primary and secondary sales of NFTs in the marketplace with differing transaction costs depending on how the marketplace operates and who facilitates the sale.

With NFTs expanding into the mainstream consciousness, what are some key legal, policy and regulatory considerations you need to be aware of?

Key legal considerations when building an NFT marketplace

- **Formation:** You'll need to form a corporate entity before launching a marketplace. This will offer your business the most substantial liability protection, greater ability and credibility when seeking financing from external sources.
- **Conduct Code:** Most NFTs, given the predominance of user-generated content and transactions in NFT marketplaces, include an extra layer of legal restrictions in the form of codes of conduct to govern interactions on the platform.
- **Smart Contracts:** The unique digital creation must be independently identifiable, with ownership transferable within the smart contract. Creators should design-in the economics of trading: How much for a primary sale, how much for secondary sales, royalties, transaction costs and other features of the aftermarket to enable trading, with funds flowing to the appropriate parties by design.
- **Platform Terms of Service:** NFT marketplaces must have essential documents such as Terms of Service, which govern the relationship between the NFT marketplace operator and customers, and between the buyers and sellers of the NFTs featured on the platform. A well-thought-out terms of service agreement can help protect your organization from various legal issues and generally have provisions limiting the company's overall liability.

- **Terms of Sale:** Sellers or creators listing their NFTs on an NFT marketplace may wish to impose additional terms of sale on purchasers of their NFT, especially if the platform's terms of service do not sufficiently address risks to the seller or creator.

- **Intellectual Property Protection:** It is vital to verify each participant's intellectual property rights through each step of every NFT transaction. Be sure to allocate intellectual property rights between the creators/artists, purchasers/collectors, and other parties involved. The ownership of the original work is copyright ownership, which vests in the creator of the original work. If an NFT is minted and sold, the purchaser will receive a set of intellectual property rights from the creator as part of owning the NFT. The seller of the NFT determines the rights that accompany an NFT. When examining the ownership of the content that you are seeking to tokenize, consider the rights of ancillary parties: Is there a record label, a studio, a sports franchise that has the right to participate in the monetization of the content?

- **Securities law compliance:** To ensure your newly minted token does not have the characteristics of a security, it's crucial to design features that demonstrate the distinction between your NFT and what governments seek to regulate. For example, the proceeds of the primary and secondary sales should not be used to build other NFTs, the platform or the marketplace. Since currency is fungible, this requires careful planning.

- **Payments:** If payments are processed on behalf of counterparties, the party touching the money may be a "money transmitter" with its activities governed by applicable Treasury, state and local registration regulations. To avoid the complex process of registration in innumerable jurisdictions, many marketplaces partner with already-registered entities, acting as content creators rather than payment processors. But watch for commissions, gas fees and other transaction costs associated with validating transactions and processing payments. How is each payment characterized? Is it a fee for content creation or money transmission? This is a key question for compliance

- **Consumer Protection:** Most major jurisdictions have laws to protect consumers. Suppose an NFT marketplace adequately fails to inform its customers about what they are purchasing and the risks involved. The FTC may then argue deceptive or unfair advertising, which may lead to hefty fines. NFTs likely will be targeted by cybercriminals for financial gain. Your platforms will need robust controls to guard against such risks. You may also need to implement KYC, anti-money laundering, and other regulatory requirements.

- **Data Privacy:** Being transparent about your data collection and use is critical. Many jurisdictions require platforms to disclose their data practices in a privacy policy. The fines for privacy violations can be significant.

- **What else is in the kitchen sink?** The existing regulatory and legal environment was not designed in anticipation of the rapidly evolving metaverse, where digital assets predominate. Nonetheless, some key issues have emerged while investors, financial and fintech companies explore this space. Is there a gateway to your platform to protect from money launderers and bad actors subject to government sanctions?

- **Show me the money:** With each piece of content, and each media in which it is reproduced or tokenized, a different license fee may be payable to a different entity in the stream of commerce. Consider whether an album cover or a musical recording is subject to royalty streams to recording labels, agents, libraries or artists, and whether a payment is due only upon the initial sale or upon each subsequent resale in the after-market. Analyzing each contract involved in the monetization of content is a key task, and care should be taken to follow the trail through each transaction in the metaverse.

Bringing it all together

If the last two years have taught us anything, it is that technology paradigms shift faster than the speed of law, policy and regulation. While contracts between two parties can be made and amended in a split second, the legal regime that governs does not always keep pace. Like all things, however, eventually the law, policy and regulation catch up. Sometimes, they land in unexpected places not envisaged at the time of contract. This checklist should help those involved in creating NFT marketplaces navigate the legal metaverse.

As marketplaces race to meet demand for NFTs, what are the legal issues at play?

Authors: **Louis Lehot | llehot.foley.com, Catherine Zhu | czhu@foley.com**

This article was originally published on The Fashion Law on September 23, 2021.

In what has proven to be a striking rise over the past several months, non-fungible tokens ("NFTs") have captivated the art world and have since entered the world of fashion, creating a market where digital versions of garments and accessories that are linked to unique blockhain-hosted tokens are increasingly coming front and center. With the sheer success of NFTs in the art world, the adoption of these relatively novel digital assets by fashion industry entities seemed inevitable, and they have quickly infiltrated everything from streetwear and high fashion to footwear and the beauty space.

Amid this blockchain-enabled revolution, key moments stand out. For example, in March auction house Christie's sold "The First 5000 Days," an NFT collage by American digital artist Beeple for the cryptocurrency equivalent of $69 million. RTFKT (pronounced "artifact") has also made a new for itself by way of its hot-selling digital sneakers and recently, a digital "Metajacket" jacket that sold for upwards of $125,000. Following the debut of these headline-making NFT-linked artworks in the market early this year, global luxury giants and fashion start-ups have similarly started looking to NFTs as a way to attract digitally-connected consumers and potentially generate revenue. There is revolutionary currency in NFTs and other forms of digital fashion (particularly for emerging designers and fledgling businesses), after all, as both types of digital assets allow newcomers to prosper outside traditional industry parameters.

All the while, marketplaces are launching (quite successfully in cases like OpenSea, which nabbed a valuation of $1.5 billion in July, and facilitation two million transitions in August, totaling $3.4 billion in trading volume for the month) specifically to capitalize on this growing demand for buying and selling NFTs. But given that NFTs are still relatively new, regulation in this area is still evolving. Given the quickly-changing nature – and the readily-growing size – of the NFT market, it is paramount to understand all the legal considerations when launching an NFT marketplace, including documentation, intellectual property, and other legal concerns, as well as overarching legal implications of this new technology.

Essential Legal Documentation

Company Formation – Launching an NFT marketplace? It is highly recommended that before doing so, the marketplace founders form a corporate entity first, as this offers the most robust liability protection for business owners and shields personal assets from business obligations. Additionally, a corporate entity provides greater ability – and credibility – when seeking financing from external sources and more flexibility to accommodate growth. To begin down this path, a company must be formed and registered correctly.

Terms of Service – A company's terms of service act as the governing legal contract between the company and its users, and thus, serve as essential legal documents. When well-drafted, they will protect the company and limit its overall liability, implement an arbitration process, and set up an indemnification framework that will cover the company in the event of any disputes.

For NFT marketplaces, putting these protections in place is vital. In contrast to SaaS or another digital product, in which a company directly provides a service to its users, NFT marketplaces usually consist heavily of goods created by third-party users, and interactions and transactions between users. Therefore, there is a higher probability that misconduct by one user will negatively impact another. In that situation, the company or the marketplace is easy to blame for anything that goes wrong, making relevant terms of service particuarly critical.

Code Of Conduct – Given the predominance of user-generated content in NFT marketplaces, NFT marketplaces are generally encouraged to include extra layers of legal restrictions specifically in the form of community standards (otherwise known as a code of conduct) to govern interactions on the platform.

Privacy Policy – Finally, privacy policies are legally mandatory. A company is legally required to disclose its data collection and use practices, among other legally required disclosures. Depending on the applicable privacy law framework (e.g., GDPR, HIPAA, CCPA), additional disclosures may also be needed.

Intellectual Property Considerations

When creating an NFT marketplace, it is vital to allocate intellectual property rights between the artists/creators, collectors/purchasers, and other involved parties fairly and effectively. Without an effective allocation of intellectual property rights in place, operators risk undermining the legitimacy of their marketplace. (It is worth noting that acquiring an NFT does not automatically transfer ownership of the original work and corresponding intellectual property rights to the buyer unless otherwise specified by the creator; ownership of the copyright in an original work, including an NFT, for instance, vests in the creator of the original work.)

The specific allocation of intellectual property rights that takes place when a party acquires an NFT from its creator is typically determined in advance by the creator. Nonetheless, marketplace operators should keep in mind that overly aggressive transfers of creators' rights may turn away artists and other creators from utilizing a marketplace. In contrast, not allocating sufficient intellectual property rights to collectors, the company, etc. will mean that the involved parties will not have the right to carry out their role or function in the marketplace.

Securities Law Considerations

Following the internationally coordinated crackdown on the initial coin offering ("ICO") craze that culminated in the Telegram payment platform's shutdown and return of $1.3 billion in ICO proceeds, issuers of NFTs and NFT marketplaces would be smart to avoid falling into the same potholes as their ICO predecessors. Wishful thinking will not prevail over securities regulators, particularly if retail investors lose all or a material part of their investment.

While each NFT should be analyzed for compliance based on its specific characteristics and the methods it monetizes, NFTs that underly collectibles (such as individual pieces of artwork) arguably should not be deemed to be securities. Instead, these NFTs are essentially finished products whose value is determined at a sale made directly to a buyer. Moreover, for NFTs representing a specific underlying asset or collectible, there is typically no expectation or need for a third party to extend organizational efforts that will enhance the value of the NFT, the sine qua non of an "investment contract" outlined by the U.S. Supreme Court (commonly referred to as the *Howey* test).

This logic has been previously supported by the U.S. Securities and Exchange Commission. In 2019, the securities and stock market regulator published a digital securities "framework" document, where it stated that "[p]rice appreciation resulting solely from external market forces (such as general inflationary trends or the economy) impacting the supply and demand for an underlying asset generally is not considered 'profit' under the Howey test." Therefore, the reasoning goes that the fact an NFT can rise and fall in value does not make it a security.

However, promoters of NFTs would be wise not to take this to the bank. Technological developments driving demand for NFTs could lead to a whole new world of derivative digital property rights that fail other Howey test prongs. The tokenization of insurance coverage and the after-market, for example, provides a notable example – artists selling rights to future proceeds on a secondary market in one form or another.

For any issuer of an NFT, an analysis must establish that a specific NFT is not security nor making a market in a security that would require registration or an exemption from registration under U.S. securities laws.

Similarly, NFT marketplaces need to ensure that they are not required to register as a securities exchange or alternative trading system and broker-dealer.

Still yet, issuers of NFTs must take care not to market their NFTs for potential appreciation, profit, or dividends. The mere marketing of an NFT could transform it from a non-security into a security. Also, issuers should avoid (and NFT marketplaces should prohibit and prevent their users from): (1) Marketing an NFT as part of a fundraising effort to build a network or platform for future sales; (2) engaging promoters, sponsors, or third parties to drive the NFTs' appreciation; and (3) enticing purchasers with the prospect of capital appreciation of the digital asset or profit linked to the efforts of the creator or other third party.

Taxation

Finally, there are additional legal implications to consider when it comes to NFT marketplaces, including taxes. In general, the IRS considers NFTs, like any other digital asset, to be "property," and anyone engaged in their sale or purchase could be obligated to pay sales tax, losses, and capital gains taxes on them. Therefore, NFT marketplace should have mechanisms in place for collecting and remitting sales taxes and documenting sale prices, commissions, and other fees accurately.

From a tax standpoint, NFT marketplaces may also have to deal with different jurisdictions' regimes, thereby, requiring heightened insight.

What Does the Future Hold?

With the current proliferation of NFTs and NFT marketplaces, which shows no sign of letting up any time soon, NFTs are positioned to allow artists and creators to monetize their work and create new revenue streams that were previously unimagine. At one point, NFT fashion items, for instance, were dismissed as a fleeting fad, but in the time since, these blockchain-based assets have secured the stamp of approval from the world's top luxury houses. Gucci, for one, sold its first NFT on June 3, 2021, offered as part of "Proof of Sovereignty," a Christie's-curated NFT sale that launched on May 25.

Other brands have also started experimenting with NFTs, using the tokens to unlock new digital products, distribution models, and monetization strategies. A couple of years ago, Nike patented the process behind its Crypto Kicks, which combined the use of NFTs with the ability to collect and customize sneakers.

All the while, many others view the current NFT craze as a bubble, with some investors buying NFTs as a speculative investment in hopes of flipping the tokens at a much higher price to make a quick profit. However, given the potential application of NFTs and underlying blockchain technology to a variety of real-world transactions, such as real estate, art and collectibles, retail, finance, and others, this tech trend is likely only at the very start of the possibilities for what NFTs can be used for in the future.

Flipping your business into the United States: Meet the Delaware C Corporation

Authors: **Louis Lehot | llehot.foley.com, Alexander Ravski | aravski@foley.com**

This article was originally published on Foley.com on October 6, 2021

A company "flip" has become a ubiquitous method of accessing the U.S. markets, whether for fundraising or commercial growth. A "flip" involves formation of a corporation in the United States, typically a Delaware corporation taxed under subchapter C of the Internal Revenue Code (a "Delaware C corp"), and transacting with your home country company, rendering it a subsidiary of Delaware C corp, with the goal of attracting U.S. investors and customers.

Delaware is most often the best choice for new startups, whether the business is born in the United States or elsewhere. Forming a Delaware C corp offers many benefits, such as access to venture capital and other private financing markets, as well as a step along the path to one of the world's premier stock exchanges, with access to deep and diversified pools of capital and future liquidity. Delaware also offers a more standardized and comprehensive body of law, allowing for legal and compliance predictability. Investors, private equity firms, and venture capitalists typically prefer (if not always prefer) for the company they invest in and conduct business with to have its domicile in Delaware. When a non-US based company grabs the attention of a US based investor, it is frequently asked to do a "flip" into Delaware in order to facilitate investment into the entity.

So How Does a "Flip" Work?

In a "flip," a non-US based company ("HomeCo"), whether based in Europe or elsewhere, creates a new Delaware C corp, or "Topco." The stockholders of HomeCo contribute shares in HomeCo to Topco in exchange for shares of Topco, and become shareholders in Topco. HomeCo becomes a wholly-owned subsidiary of Topco, and TopCo becomes the parent of HomeCo, with all shareholders and assets moving into that entity.

Similarly, HomeCo can contribute its assets to TopCo in exchange for shares, and the legacy HomeCo shareholders can thereby become indirect shareholders in TopCo through their continued holdings in HomeCo. This transaction frequently triggers a taxable event for HomeCo, which can be advantageous if done early, and costly if done later.

In another twist, HomeCo can license its intellectual property and know-how to TopCo in exchange for shares of TopCo, or for a license fee.

Below are some considerations for owners when debating whether a "flip" is a fit for their company:

- Consider tax implications resulting from how the technology will be either shared or sold from one entity to the other via a licensing agreement or sale agreement, respectively.
- Can the Delaware "flip" be accomplished on a tax-free basis?
- Ensure that the share exchange between HomeCo and Topco is completed in the same proportion as the way in which shares are held in HomeCo. It is important not to treat shareholders differently in this case.

- A non-US based company will stand to benefit tremendously if it conducts a "flip" in the early stages of its operations. The longer the non-US based company waits, the "flip" will become more costly and legally complicated.
- Consult local tax and legal professionals of the jurisdiction where the non-US based company is incorporated.
- Are executives and stockholders also relocating as part of the "flip"? If so, consider whether an exit tax will be applied by the home country. France is well known for imposing an exit tax on entrepreneurs expatriating and flipping to third countries.
- A share exchange agreement must be entered into by each shareholder of the non-US based company and the US company.
- Shares are not usually available immediately, as there is a waiting period in non-US based countries to register shares in Topco.

Tax Considerations

The tax consequences of a "flip" are complex, and shareholders may want to seek the advice of tax advisers before a "flip." To the extent possible, an adequately structured "flip" should be tax neutral to the non-US based company and existing shareholders and should generally preserve the current tax benefits enjoyed by the non-US based company and its shareholders.

Once the "flip" is completed, if Delaware is chosen, the Delaware corporation will be a holding company absent of operations, and its sole asset will be 100% of the share capital of the non-US based company.

A Few Disadvantages

If Delaware is chosen, a Delaware holding company structure has its benefits and also its drawbacks, such as:

- There can be tax implications of the "flip" that require further detailed analysis. A company's failure to comply with the precise requirements may result in valuable tax benefits or create other consequences.
- By forming a parent company in Delaware, the company could become exposed to the risk of litigation in the US earlier in the process than would otherwise be the case.
- US corporate and income taxes will apply to your new entity.
- Delaware applies a franchise tax to corporations.
- Individual states where a permanent establishment is maintained will also apply income, sales and payroll taxes.
- Litigious environment for doing business.

A "flip" is a popular transaction for non-US based companies that seek US based investment; however, it is not to be entered into without careful consideration. While a "flip" can provide a promising route to new financing and increased shareholder value over the long term, the non-US based company's management team should consider if a "flip" truly makes sense in the early stages of the company's financing lifecycle.

Careful consideration should be given before "flipping" to a Delaware LLC. The LLC offers many tax efficiencies, but complexities abound, particularly when attempting to raise funds from tax-sensitive investors, or compensating local talent.

A "flip" is only one avenue among many for non-US based companies when considering how to access US markets.

Meet the new SPAC circus ringleader: the PIPE investor

Author: **Louis Lehot | llehot.foley.com**

This article was originally published on louislehotattorney.com on September 2, 2021

Since late 2019, when the special purpose acquisition corporation, or SPAC, returned to the public markets with a new twist, a circus of activity has breathed new life into the markets for privately-held emerging growth companies, forcing open a large window for public exits not seen in decades.

In this "SPAC 2.0 boom," sponsors of SPAC vehicles first raised large pools of blind capital in the public markets and then strutck deals to buy emerging growth companies for ~10x the cash raised plus rollover equity and a second pile of cash in the form of a PIPE.

What is a PIPE, and why is it used for a de-SPAC merger?

"PIPE" stands for "private investment in a public entity," often priced at a discount or containing a "sweetener" for the PIPE investor to make a more significant commitment than it would otherwise in the public market.

The PIPE fundraising process happens after an LOI for a de-SPAC is signed, but before a definitive merger agreement, and is signed and announced concurrently with the latter. Then the SPAC and the target work together to prepare a joint registration sttatement and proxy filing on Form S-4 and seek SPAC stockholder approval, which requires the U.S. Securities and Exchange Commission to review and clear the de-SPAC transaction.

Once the de-SPAC merger closes, the company files a resale registration statement to register the shares of common stock and warrants underlying the PIPE.

PIPE investors include investment funds, hedge funds, mutual funds, private equity funds, growth equity funds, and other accredited large institutional and qualified institutional buyers of publicly traded stock. The PIPE is well suited to complement the SPAC in a de-SPAC merger because of the speed of execution and because it does not require advance SEC review and approval.

SPACs have tapped PIPEs to bring in additional capital in a shorter amount of time to close de-SPAC mergers. Because of the nature of the SPAC process, there is often uncertainty surrounding the amount of cash that will be on hand following the merger. When combined with the SPAC proceeds in trust, the funds from the PIPE work together to provide liquidity for sellers and post-closing capital for the business to grow.

To be clear, in SPAC 2.0, the enterprise value of the target is so many multiples of the SPAC proceeds in trust that a PIPE has become ubiquitous to bridge the value gap. The Morgan Stanley data showed that on average, PIPE capital almost tripled the purchasing power of the SPAC, and for every $100 million raised through a SPAC, adding a PIPE added another $167 million.

Raising funds via a PIPE deal is comparable in some ways to an IPO roadshow in that there is a pitch to potential investors. However, PIPE deals are only open to accredited individual investors, and the share price is determined by reference to the de-SPAC merger valuation.

When looking for PIPE investors in SPACs, targets look for high profile names whose investment at a specified helps to validate the deal. This investment by well-respected investors can help to mitigate some of the risks that come with SPACs.

> *"PIPE investors include investment funds, hedge funds, mutual funds, private equity funds, growth equity funds, and other accredited large institutional and qualified institutional buyers of publicly traded stock"*

While PIPE deals are seen as an attractive option partly because they avoid many SEC regulations, all the attention SPACs have received, and their incredible spike in popularity has drawn the attention of regulators. This could mean additional regulations are on the horizon for both SPACs and PIPEs. But for now, these two continue to be an attractive combination for those looking to bypass the traditional IPO process.

What is SPAC 2.0 and why is the PIPE investor the ringleader?

SPAC 2.0 was essentially the cash in the SPAC vehicle combined with a new private fundraiser in the form of a PIPE merged into a privately-held emerging growth company. The resulting party for SPAC IPOs, de-SPAC transactions, and even traditional initial public offerings, or IPOs, continued through the end of the first quarter of 2021, with hardly even a little intermission for the first COVID lockdown.

According to data compiled by Morgan Stanley, in 2020, PIPEs generated $12.4 billion in additional funding for 46 SPAC mergers. The SPAC 2.0 structure had something for everyone:

- the emerging growth company got a public exit without having to go through a traditional IPO
- the emerging growth company stockholders got a snap spotvaluation based on three-year out financial projections not available in conventional IPOs
- the emerging growth company got a public acquisition currency in the form of listed stock, validation in the public markets via the stock exchange listing, and cash to the balance sheet to power growth
- stockholders in the emerging growth company could negotiate for some amount of immediate liquidity
- stockholders in the emerging growth company got long-term liquidity via the =public trading market
- SPAC stockholders and PIPE investors got access to emerging growth companies that weren't otherwise going public
- SPAC sponsors made their "carry" in the form of 20% of the equity in the SPAC (pre-dilution) plus warrants in some cases and a path to liquidity with a short lock-up period
- SPAC sponsors could rent out their names, network, and prestige and get a quick exit

While in SPAC 1.0, the SPAC sponsors would take over the target and operate it like a private equity buyout fund for long-term capital growth, in SPAC 2.0, the SPAC sponsors are like bankers, raising capital and then handing over the keys to management of the emerging growth company in exchange for a commission.

But the lights went out for the SPAC party in April 2021 when President Biden appointed a new chair to lead the Securities and Exchange Commission. Upon taking office, new SEC Chair Gary Gensler effectively closed the market for SPACs by announcing a compliance review, putting long-standing SEC policy and rule interpretations in doubt. Transaction participants reported that SEC staffers reviewing their pending transactions started asking questions, requesting changes, and appeared in no hurry to clear pending "de-SPAC" deals.

The market for new issues froze up, and the demand for de-SPAC transactions ground to a halt. The trading index for recently "de-SPAC'ed" public companies dropped double-digit percentage points. Investors started to lick their wounds.

"The amount of capital PIPE investors are willing to put into a de-SPAC transaction at a given valuation and what sweeteners have become the deciding factor as to whether a de-SPAC transaction can get done"

When the SEC began clearing SPAC mergers again in early summer 2021, it was not as simple as just turning lights back on and taking its foot off the brakes. That is because PIPE investors, who provide fresh capital to the company that is merging with a public SPAC vehicle (commonly referred to as a "de-SPAC transaction"), have taken their place as the new ringleaders at the SPAC circus.

The amount of capital PIPE investors are willing to put into a de-SPAC transaction at a given valuation and what sweeteners have become the deciding factor as to whether a de-SPAC transaction can get done.

PIPE investors no longer accept transaction terms as proposed and have started to make new commitments contingent on adjusted valuations, redemptions of SPAC sponsor promote securities, and better alignment to create better after-market trading conditions.

Knowing what PIPE investors want and how much they will pay has become the new ticket to success in the SPAC market. This makes the PIPE investor the new ringleader in the SPAC 3.0 cycle.

Looking into the future of a legal metaverse?

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on Venture Beat on September 1, 2021

Initially coined in 1992 by Neal Stephenson, the term "metaverse" comes from his sci-fi novel, *Snow Crash*, in which humans interact with each other via avatars rendered in three-dimensional virtual space.

As Matthew Ball, the former head of content at Amazon, stated, "The metaverse is a persistent, synchronous and live universe that spans both the digital and physical worlds with total inclusion." It is described as a digital shared space where everyone can interact seamlessly in a fully immersive, simulated experience. It is the increased permeability of the borders between different digital environments and the physical world. In the metaverse, you can interact with virtual objects in real life with real-time information. A mixture of what is virtual and what is real. A place where people join together to create, work, and spend time together.

It should come as no surprise that tech giants are already all in and building in the metaverse. Games' Fortnite, Microsoft's Minecraft, Facebook's Horizon, and many more are contributors. In fact, Facebook's Mark Zuckerberg laid out his vision to transform Facebook from a social media network into a "metaverse company" in five years. "This is going to be the successor to the mobile internet," Zuckerberg told shareholders this month. "You're going to be able to access the metaverse from all different devices and different levels of fidelity from apps on phones and PCs to immersive virtual and augmented reality devices."

How to engage, work and play in the metaverse

The different types of activities that will take place in the metaverse are limitless. For example, think about COVID-19, where events such as happy hours, weddings, school classes, and work were increasingly taking place with users participating digitally regardless of their actual geographic location. The metaverse presents the opportunity to leverage remote work even further. Virtual conferences and a plethora of tools specifically designed to facilitate collaboration by distributed teams have already come into play.

The metaverse will further offer fully immersive gaming experiences exceeding current Virtual Reality product offerings tenfold. The gaming space seems especially likely to play a role in bringing the metaverse to fruition since video gamers already own some of the most robust computational processors available.

Investing in the metaverse

Companies are continuously trying to up the ante and keep us engaged and entertained.

The "metaverse" is the newest chapter in entertainment, and its growing popularity means investors should at least be familiar with it.

Every day the sector is growing. It's still unclear what the metaverse will look like, but according to research firm Strategy Analytics, the global metaverse could be worth $280 billion by 2025 and likely grow from there. This market forecast amplifies the interest in metaverse companies bringing new ways to interact with users, which intersects with a world spent indoors and a rise in technological capabilities available to innovators.

How does the metaverse change the legal system?

The metaverse is upending our legal and regulatory systems and begs the question of who makes and enforces the rules.

Life is not a game, however. And when you apply old rules to new technology, you will find yourself trying to put a square peg into a round hole. But here goes it:

- **Intellectual property:** when one or more players in a virtual game collaborate to create a virtual good or a virtual world, who owns it? Is it copyrightable? Is it possible to create, protect or enforce a brand inside a virtual world? What strategies can content creators deploy to protect their brands within the virtual world? This is particularly important for consumer-facing businesses.
- **NFTs:** we have all witnessed the cottage industry of value created through tokenization of entertainment, sports, and media personalities and teams through tokenization of non-fungible content. While today the media is focused on entertainment and media content being tokenized in the metaverse, imagine when entire towns, cities, regions, countries, and superstates are created virtually, with the resulting explosion of content. In other words, we have only begun to see the metaverse commercialized through NFTs. Are they securities? Are they currencies? Who regulates? Who can purchase? Who can trade?
- **Data protection and privacy:** as humans spend more and more of their waking (and sometimes sleeping) hours in the metaverse, who owns the resulting data? Who is protecting your identity? What happens if your information or identity is misappropriated? Who is responsible?

These are just examples of the many conundra emanating from the question of who makes the rules and enforces them. Some say that there should be an attempt within every legal system to adapt to the metaverse. Others back the creation of a new legal system specially designed for the metaverse. While the metaverse holds great promise for merchants and investors alike, without a system for design, promulgation, and enforcement of rules, it could be dangerous. For now, the metaverse has been growing in a virtual sandbox. How long will this last? Until the first Meta-tragedy that captures public attention? Or will someone or something lead the charge? The crypto world provides a valuable indicator of what happens when rulemaking remains fully decentralized.

Is a metaverse world far off?

A true metaverse may still be a few years away.
In the meantime, Facebook and other pioneers are busy laying the groundwork for a future that permits families, friends, coworkers, and more to meet and interact in shared digital spaces that look and feel authentic. Digital currencies will also be essential.

The metaverse world is in play, and that which is existing separately is gradually coming together. Technology is not proficient enough to support this integrated metaverse just yet, and the reality of its adoption might be a while away. However, the metaverse has the backing of billionaires, talented game designers, and the only rival to the metaverse is life itself.

Louis Lehot is an emerging growth company, venture capital, and M&A lawyer at Foley & Lardner in Silicon Valley. Louis spends his time providing entrepreneurs, innovative companies, and investors with practical and commercial legal strategies and solutions at all stages of growth, from the garage to global.

The future of virtual deal-making and the return to work

Author: **Louis Lehot | llehot.foley.com**

This article was originally published on Venture Beat on May 6, 2021

Over the last year, the pandemic upended many industries, prompting businesses to pivot quickly to enable a fully virtual everything, from workplace to marketplace to nearly every aspect of life. Even the legal profession, which historically has been slow to adopt technology, is now starting to catch up to other industries by embracing digital transformation. The results in the startup world have been similar to those seemingly everywhere else. In-person meetings have been scrapped in favor of virtual meetings. Travel has been replaced by videoconferencing. Paper has been replaced by bits and bytes. While the tech industry is starting to return to normal, how much the new normal will be like the old is still an open question. At the same time, increased reliance on technology is changing the trajectory of virtual deal-making.

The rapid virtualization of many business functions has had a number of unintended consequences. On the one hand, for startups and investors, virtual deal-making has become commonplace, which has changed the dynamics of raising capital and investing. One startup CEO noticed that compared to pitching in person, virtual deal-making had a heightened focus but found that "it allowed for more robust conversations and data sharing over a shorter period of time." This pattern has been common since COVID-19 pushed so many meetings into cyberspace, but it also particularly complements high-resolution fundraising, allowing startups to connect quickly with more investors than ever before.

By driving faster connections and more pitches, these virtual meetings seem to be working well for the industry. Despite the pandemic, 2020 was a banner year for venture capitalists, with a record-setting $130 billion invested in over 6000 deals.

But on the other hand, virtual deal-making has some significant drawbacks. Many people across all industries are tired of videoconferencing. We even have a genericized term for that now: "Zoom fatigue."
As Stanford University noted, virtual meetings face significant challenges compared to in-person meetings, specifically relating to cognitive load, a lack of movement, and too much screen time.

Where will the industry go from here? As businesses open up more and travel becomes more normalized again, in-person deal-making will probably stage a staggered return. Many people prefer them, so they will always be good fits for some. But given the changes in the past year and the benefits that many saw from faster pitch cadences, startups and investors will probably continue making deals virtually, almost certainly more than they did back in 2019 and prior, which leaves a big question about addressing the challenges of virtual meetings.

Companies have delivered annual and quarterly financial returns with a largely steady topline and bottom line benefiting from elimination of the travel and entertainment budget. With the economy returning to work, spending on travel and entertainment will return, but at what pace and in what quantum? Will cost savings be retained when growing the topline with a workforce back at full capacity?

I'll end with one possible (and admittedly speculative) solution, at least in part. For many years, dating back at least to the 1990s and the early days of stereoscopic video games, virtual reality (VR) has been touted as the next big thing. And yet, even the 3D-television craze several years ago and the rampant interest in VR headsets has not led to significant adoption. While we may see VR find a place in high-level business meetings, augmented reality (AR) appears better positioned to make significant inroads.

New augmented reality technologies that enable meeting participants to not only see each other and share documents, but immersively view, manipulate and interpret data together in an augmented, three-dimensional or phygital world, could be a game changer. For a sneak view of what an augmented reality, augmented data analytical world would look like, check out what our friends at Flow Immersive are building here, or the "phygital" worlds built for clients of Double-A Labs.

AR could enable virtual meetings while also providing more natural interactions than staring at a screen would allow. Maybe bridging the gap between the virtual and real worlds would be enough to address the fatigue that so many feel with virtual meetings.

The ability to have more natural interactions with clients, business partners, investors, and lawyers without the cost (or risk) of travel could be a major deciding factor to pushing AR meetings into the mainstream. A number of companies are working on related technologies, so the question is who will make it work first. Maybe someone will come up with an entirely different and vastly superior solution. Time will tell.

How major automakers and aircraft manufacturers are moving fast to innovate with smart strategies and big investments

Author: **Louis Lehot | llehot.foley.com**

This article was originally published on LouisLehot.com on August 13, 2021

The future of the auto industry has arrived, driven by technological advances that once seemed to be only science fiction. This technology, combined with an increased focus on sustainability, has led to a boom in investment in startups by major automakers.

Today, automakers are increasingly funding startups producing next generation batteries and electric vehicles, technology related to autonomous cars and trucks, as well as electric aircraft. According to data from Crunchbase, automakers led $9.6 billion in private funding rounds for startups since the beginning of 2020.

This investment by automakers is being spurred by a need to invest in the future, expand their tech capabilities and capitalize on the transformation of the industry. Some automakers choose to innovate in-house, however, those who choose to invest in startups can still achieve these goals and contribute to industry innovation without using up all their R&D budget. They can also cast a wider net and help to minimize risk.

Crunchbase reported that since 2020, Volkswagen has been the most active automaker investing in startups, participating in 24 deals, with the largest concentration of funding in batteries. They were the lead investor in $3.4 billion in funding for Northvolt, a Swedish company that manufactures lithium-ion batteries.

Crunchbase data also showed that Toyota came in second place, participating in 20 deals since 2020 and leading a $590 million Series C for electric aircraft maker Joby Aviation. Toyota has stated their VC fund is investing in startups that help them refine processes, improve supply chain management and bring better robotics to their factories.

BMW recently announced the creation of their BMW i Ventures Fund II, with $300 million to invest in early and mid-stage autotech startups. The fund focuses on sustainability, as well as transportation, manufacturing and supply chain. BMW i Ventures has already invested in over 50 early and mid-stage startups since it was created in 2016.

Truck rental company, Ryder, has even launched a VC fund, Ryder Ventures. The fund invests in “innovative companies creating the technology and applications that will drive the industry forward.

This includes next generation vehicles, supply chain automation and e-commerce fulfillment.

We have seen something similar in the tech sector as the tech giants invest in the up and coming startups developing cutting edge, innovative products.

While purchasing minority stakes in promising startups is one way to get exposure to technology, automation, clean energy and autonomous driving, some automakers are doing this by forming joint ventures.

For example, Volkswagen also announced in July the formation of a joint venture with Croatian based startup Rimac[1] (formed by Mate Rimac in his garage in 2009) with its Bugatti brand to create a new electric supercar.

> *Some automakers choose to innovate in-house, however, those who choose to invest in startups can still achieve these goals and contribute to industry innovation without using up all their R&D budget.*

Rimac Group will continue to develop, produce and supply battery systems, drivetrains and other EV components through Rimac Technology. Rimac Group is backed by Korean auto-manufacturer Hyundai Motors and Germany's Porsche.

In China, Geely has been actively acquiring stakes in other global automotive manufacturers and bringing technology and products back to China. China has committed to an electric vehicle fleet inside of this decade and is sprinting to meet this goal.

The aircraft sector is not to be outdone by the automotive sector. In August 2021, Boeing announced plans to spin-off its venture capital arm, HorizonX, to forge a broader investment fund.

As part of the deal, Boeing will partner up with AE Industrial Partners (AEI), a specialist private equity firm, and other third party capital providers, to broaden the investor base, access more outside innovation and develop new technologies.

Boeing's archrival Airbus maintains its own captive venture arm with global operations. Each of Boeing and Airbus have deployed hundreds of millions of dollars into startups in the past several years, and are expected to continue their rivalry here, albeit now using different strategies.

The private and public capital markets are working hand-in-glove with the automakers and aircraft manufacturers.

Special purpose acquisition corporations have been formed, raised and transacted with industry players to forge newly public vehicles to disrupt the transportation space, from Virgin Galactic to JOBY Aviation. The SPAC 2.0 product has enabled public financing of vehicles that were previously thought to be unfinanceable, enabling whole new ways of transporting people and cargo.

Others are looking to provide alternative sources of capital to startups based on the assets produced rather than the purported value of the enterprise. Case in point: former helicopter and fixedwing operator lessor and lessee Hooman Yazhari has formed Mobility Capital2 to deploy non-dilutive assed-based financing to enterprises developing the next generation of the mobility and transportation economy.

Rather than invest in the companies building technology, Mobility Capital aims to finance the production and sale of the transportation vehicles themselves.

As technology continues to disrupt and transform the automotive, aircraft and transportation industries, we can expect to see a continuation of manufacturing giants investing in startups and partnering with other sources of capital to create the economy of the future.

With electrification of the global fleet of automobiles and aircraft in full swing, autonomous driving may not be far behind. The financial markets are working with manufacturers to accelerate technology leaps required to get there.

Notes

[1] https://tcrn.ch/3m0Kbux 2 https://bit.ly/3iFUMt1

The rise of Central-Bank Digital Currencies: A primer on CBDCs

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on Medium.com on July 20, 2021

The Bitcoin rollercoaster has brought a lot of attention to cryptocurrencies over the past year, but you still can't pay your taxes with them. Aside from some state-level moves to accept cryptocurrencies, taxes must still be paid in the U.S. dollar. And yet, as more businesses go through their own digital transformations, many have been wondering when the economy will experience its own digital paradigm shift.

The idea of a digital dollar is not new. Digital currencies have been discussed for decades, and some even argue that the dollar is already digital. There is merit in that characterization. Most of the money in the U.S. money supply is not cash — what consumers generally consider money to be — but debt-backed derivatives of cash deposits. Since those dollars exist digitally, the dollar already is essentially a digital currency. But the recent discussions of a digital dollar revolve around creating a federally backed central-bank digital currency (CBDC).

CBDCs share some technological characteristics with cryptocurrencies, but they differ in organizational structure. CBDCs are by definition centralized, meaning that the issuer of the currency has direct control over it. In recent years, there has been more talk of CBDCs, particularly as China has pushed to become the first major issuer of a CBDC. (The Bahamas has the distinction of issuing the first CBDC — the Sand Dollar.)

China's experiment with a digital yuan has sparked both governmental and private-sector discussions of the merits and risks associated with CBDCs. One common concern with the digital yuan is the increased control that it gives to the Chinese government. Some view this control as a threat to the West, and the fear of lagging behind technologically seems to have spurred many countries to consider issuing their own CBDCs, with about 80% of central banks now open to the possibility. In the U.S., both Janet Yellen (secretary of the Treasury) and Jerome Powell (chairman of the Federal Reserve) have expressed interest in a digital dollar. Expect to hear more concrete news this summer.

Any digital-dollar initiative would likely require action from Congress, and it would also trigger a host of legal questions. For example, how would people acquire accounts? If accounts were tied to banks, the digital dollar would work only for those with bank accounts. As of 2019 (the latest data available from the government), 5.4% of U.S. households are unbanked. While that percentage is small and has been declining over the past decade, it still encompasses 7.1 million households. Would those people be prohibited from using a digital dollar?

If the digital dollar were not tied to bank accounts, the government would have direct control over transactions, which would lead to privacy concerns while also threatening the traditional banking industry. As Bloomberg reported in March, the American Bankers Association believes that a digital dollar "is a costly solution in search of a nonexistent problem," while credit-card companies are trying to make sure that they would not be cut out of any proposed CBDC.

The long-term effects on businesses are difficult to predict given the lack of concrete information at the moment. But as with any paradigm shift, there likely will be unforeseen consequences. Pay attention to developments in this space.

What to expect for cybersecurity investment as we emerge from the pandemic

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on VentureBeat on July 18, 2021

As we emerge from the global pandemic and return to robust economic growth, the cybersecurity industry is on fire and venture capitalists are taking notice. While the industry has seen steady growth over the past decade, since 2019, industry expansion has accelerated at a breakneck pace. This is particularly true when you look at industry growth and investment in 2020 and in the first quarter of 2021. We look at what's driving demand, dive into the life of a cybersecurity startup, examine target markets, and scan the horizon for signs of what's in store for the future.

What's driving interest?

Major breaches are continually making headlines, and the security risks created by an increasingly remote workforce are leading companies and individuals to rapidly increase their spending on cybersecurity protections. In fact, research firm Gartner forecasts that spending on cybersecurity will surpass $150 billion in 2021, an increase of 12.4% over last year.

Where is innovation happening?

This surge in interest in cybersecurity has led to a wave of startups popping up in this space, looking to take advantage of this incredible opportunity. According to a Crunchbase report, 2020 was a record-breaking year for the cybersecurity industry with six new cybersecurity unicorns. Just a few months into 2021, we have surpassed that record with nine new cybersecurity unicorns already.

That same Crunchbase report also noted a record year for investment in the cybersecurity space in 2020 with $7.8 billion invested globally, nine times greater than what the industry saw just 10 years ago. This year is already on pace to smash the record-breaking industry investment of 2020.

Case study: Dover Microsystems

Dover Microsystems is a case in point, a cybersecurity startup based in Waltham, Massachusetts, led by co-founder Jothy Rosenberg.

With cybercrime estimated to cost $6 trillion in 2021, a business will likely fall victim to ransomware every 11 seconds, according to Cybersecurity Ventures. A global car manufacturer recently spent a reported $2.1 billion on responding to the hack that occurred during the demonstration of a new vehicle. Customers don't know what to do, so they keep adding layers of defensive software, cluttering up their software stack and slowing down their products. This makes the problem worse: software has up to 50 bugs per 1,000 lines of source code.

Dover believes that the only way to stop 95% of attacks that come over the network is in silicon, where it cannot be subverted over the network. The result is CoreGuard, a unique, disruptive solution to the failure of cybersecurity defense across all our computing systems in all vertical market segments. It integrates with leading processor architectures to monitor every instruction executed to ensure that it complies with a defined set of security, safety, and privacy rules. If an instruction violates a rule, CoreGuard stops it from executing and notifies the host processor in real-time of the exact offending line in the source code that was exploited.

While formed more than five years ago, Dover leveraged lean capital to develop a minimum viable product, sell multiple proofs of concept, and then begin commercial shipment. Looking forward, Dover intends to sell into the B2B as well as the B2G spaces, which are markets that are forecasted to see significant growth in the coming years.

Demand triggers for the cybersecurity market

What is leading investors to pour money into the cybersecurity industry? There is an increase in demand for cybersecurity products driven by several factors.

One of the major factors is today's remote workforce. The pandemic forced companies to pivot as employees worked from home, a trend that does not look to be going away anytime soon. With a remote workforce and sensitive data moving through the cloud, there are serious security concerns. This has led to more cloud security startups looking to provide solutions to companies seeking ways to protect their data. Gartner research showed 41% growth in end user spending on cloud security between 2020 and 2021.

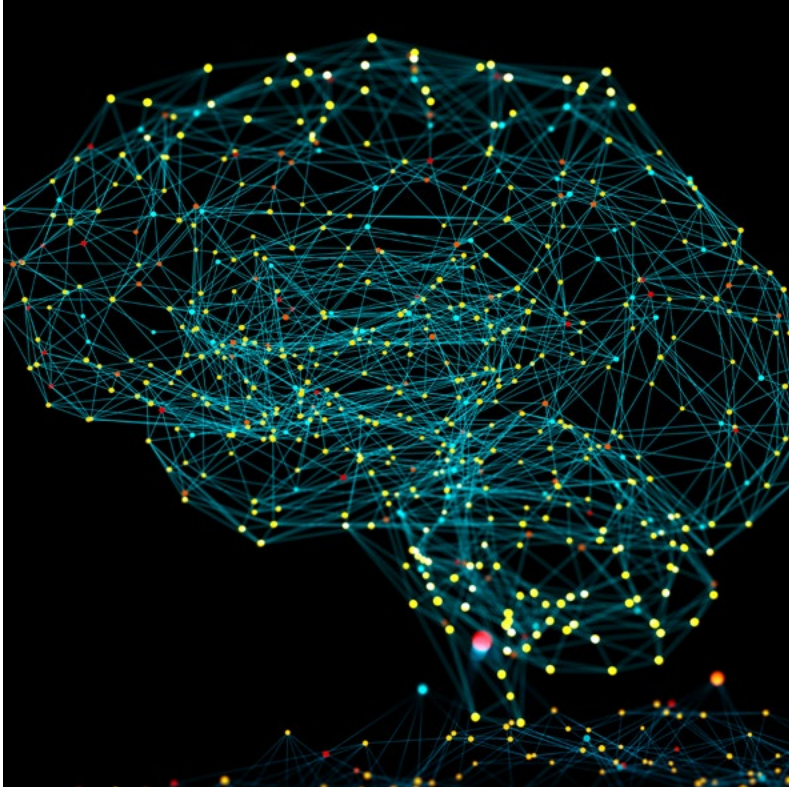
Companies are also handling more data than ever before, making them more attractive to hackers looking to steal that data or hold it for ransom. We are seeing an alarming number of data breaches and ransomware attacks facing U.S. companies. According to Risk Based Security, "the total number of records compromised in 2020 exceeded 37 billion, a 141% increase compared to 2019 and by far the most records exposed in a single year since we have been reporting on data breach activity." Already in 2021, we have seen high-profile breaches and ransomware attacks impacting the D.C. police department, the Colonial Pipeline, and meat producer JBS, and there are surely many more to come in the second half of the year.

Scanning the cybersecurity horizon

These factors have created an ideal environment for cybersecurity startups looking to offer their products, services and solutions to companies and individuals demanding greater protection. Because the demand is only increasing, investment in this area is also on the rise. The Crunchbase report highlighted the increase in deal value in just the past three years. In 2017, the average deal value was around $6.9 million. In 2020, that number jumped 73% to an average of $11.9 million per deal. This shows a greater appetite for investment in this sector that is sure to keep growing.

With 2021 already poised to outpace record-breaking 2020 in cybersecurity spending and investment, this industry will be one to continue to watch long-term.

Quantum future and the quantum arms race



Author: **Louis Lehot | llehot.foley.com**

This article was originally published on Data Driven Investor, on June 30, 2021

Quantum computing is a perennially hot topic in science and technology, with many researchers and companies scrambling to build the first truly practical quantum computer. But as with many technological advancements, the complex jargon can easily obscure the big picture. In cybersecurity, the quantum arms races consists of three fronts: quantum computers, post-quantum cryptography, and human users. With help from our friends at Aimava, we will explore these topics at a digital summit with leading thought leaders, corporations and investors on the future of quantum computing in July.

Quantum computing offers the possibility of solving problems that conventional computers cannot, at least not in a reasonable time frame. Modern information technology relies heavily on cryptography that in its current state could be easily broken with a fully functioning quantum computer.

Typically, modern cryptographic keys are created by multiplying very large prime numbers to create even larger composite numbers. Multiplying is easy for a computer, but reversing that operation—factoring—is computationally difficult for the systems that we use today.

A key can be broken if the factors can be determined. The exact cryptographic implementations are, of course, more complicated, but this basic mathematical unidirectionality underlies much of the cryptography that secures the Internet today. Obviously, security is important not just to individuals and companies but also to governments. The combined computing power of the entire planet would require billions and billions of years to crack properly implemented cryptographic keys, and the algorithms have been tested and retested for long enough that we can be reasonably sure that someone will not find a significant shortcut.

However, a quantum computer could make certain kinds of problems feasible to solve. By using the oddities of quantum mechanics, a quantum computer could (at least theoretically) factor a transport layer security key in a trivial amount of time. Again, quantum computers have many other potential applications, but cryptography is a major one with serious financial and geopolitical consequences. This is highlighted by the recent increase in cybersecurity attacks, the scale and frequency of which has significantly superseded prior records. We've seen that sophistication of attacks has increased as bad actors are able to harness new technologies such as artificial intelligence and machine learning. One can only imagine the terrifying implications for cybersecurity if these bad actors were able to apply quantum computing to their attacks.

As practical quantum computers edge closer to reality, others are developing algorithms that are intractable even for quantum computers. Given the massive implications for cybersecurity and cyberwarfare, businesses and nations cannot afford to ignore quantum computers and post-quantum cryptography. Being able to break today's common security algorithms has severe implications for security and legal compliance. It can also have devastating consequences on the business itself, including regulatory fines, costs of remedying the breach, reputational harm, and potential consumer litigation.

There has been a steady increase in the number of quantum computing startups as well as venture funding in quantum computing. On the other end, tech giants such as Intel, Google, IBM, Microsoft, and Amazon are investing resources in quantum computing technology. Google started experimenting with post-quantum cryptography in Chrome back in 2016, and PQShield, a startup developing quantum-resistant security tech, raised $7 million last year. Just recently, Honeywell and Cambridge Quantum Computing announced a new partnership to leverage their respective expertise in quantum hardware and software.

Quantum computing will be a gamechanger if (or when) it comes to market, and post-quantum cryptography is a necessity as a result. In fact, highly sensitive data should probably be migrated to quantum-resistant algorithms as soon as possible. But no matter how good encryption is, the human element is often the weakest link. It's worth paying attention to ways companies are using to make humans more secure. For example, years ago, Google started requiring its employees to have physical security keys, and since then it has not suffered a breach from phishing attacks.

In a post-quantum world, not only will technical controls be important elements of cybersecurity, but organizational measures and operational considerations will also be necessary. No matter how secure a system is, users are almost always weak points, so while the quantum arms race heats up, it will be important for companies to develop and implement access controls to make users less susceptible to security breaches. As the sophistication of bad actors increases, companies will likely need to bolster both internal and external coordination, including working with government agencies and other industry groups in collaboration.

Quantum computers, quantum-resistant cryptography, and human users will all have effects on the cybersecurity industry in the future. We have no way of knowing when a major breakthrough will come, so the best that we can do is prepare now.

As mentioned, we are co-hosting a digital summit to drill down into these topics in July with our friends at Aimava. Quantum Future will feature thought leaders, corporations and investors that are looking to scale up in quantum computing. We are looking to forward to hearing from Prem Tumkosit at Merck GHI Fund and Ilana Wisby CEO of Oxford Quantum Circuits as they share their experiences testing and deploying quantum solutions in security, new chemical discovery, pharma development, massive logistic optimization and seeing the unseen. There will be breakout sessions for attendees with facilitators including Christopher Savoie – CEO Zapata, Chris Erven – CEO, KET Quantum Security, Richard Murray – CEO Orca Computing, Daniel Franke – Merck KGaA, M-Ventures and Andy Stanford-Clark – Chief Technology Officer IBM UK, to name a few.

Rise of the machines: Two factors driving automation

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on Global Trade on June 18th, 2021

Today I want to talk a little about automation. I've talked earlier about the future of work, and there are some obvious trends like remote work and digital transformation. But automation is a significantly growing field, especially in retail markets. Trends in the industry respond to market pressures that affect the supply of and demand for labor. When human labor is cheap, automation will be used less. When human labor is scarce or expensive, automation will be used more. Today, I want to focus on two key market pressures that are driving demand for more automation.

First, declining birth rates are signaling potential labor shortages in the future. According to the CDC, in 2020, the total fertility rate (TFR) for the U.S. dropped to 1637.5 births per 1000 women, a decline of 4% compared to 2019. While some might blame the pandemic for the decrease, the 2020 number follows a downward trend that started in the 1970s. With fertility below the replacement rate of 2100 births per 1000 women, the U.S. labor force may be starting to decline. With an aging population and fewer workers, companies will likely be forced to increase automation or increase pay to attract and retain employees.

Second, rising labor costs are already encouraging companies to experiment with more automation. Depending on which pundit you ask, you will get very different answers as to why labor costs are rising now, but whatever the reason, businesses are grappling with higher personnel costs. As an article in Forbes recently noted, "The law of supply and demand says this scarcity makes existing workers more valuable, letting them insist on higher pay and better conditions." As a result, some companies are turning to automation. Fast-food chains are experimenting with automated fry cooks. The drive-thru is also poised to see more automation. Other experiments include cashier-less grocery stores and last-mile delivery.

Retail automation, therefore, seems poised for growth, but automation likely will not be a good fit for every job. Peanut the robot, for example, demonstrates that automation cannot effectively replace wait staff yet, but you may have noticed an increase in self-checkout lines in many stores. Kiosk ordering at restaurants has also been rising in popularity over the last few years, and as noted above, fast-food restaurants are experimenting with highly automated systems. In many cases, automation has the advantage of driving down operating costs. Robotic systems, for example, may have high capital costs, but they do not tire or want health benefits like human workers. Therefore, robotic systems can reduce long-term costs and save companies money.

All of these automation systems build on technology trends that have been growing for years: voice recognition, touchscreen interfaces, online shopping, and robotics, to name a few. Companies investing in these spaces will likely do well once retail automation really takes off. Some may worry that automation will eliminate jobs, but that likely will not become a serious problem. Throughout history, automation has eliminated some jobs while creating others. I recommend worrying less about the jobs that automation will eliminate and instead focusing on what new kinds of jobs will be enabled by the new technologies.

What goes down must come up: Post-pandemic trends in business and technology

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on National Law Review on May 10, 2021

Welcome to the Business & Legal Developments in Silicon Valley Newsletter, a monthly round-up of pertinent updates and articles from Foley & Lardner LLP. Today we are highlighting SPACs, NFTs and looking at another growing tech trend. The tech world is, of course, always changing, but the ongoing and rapid digital transformation driven by the pandemic is accelerating everything virtual, maybe even virtual bubbles.

Cooling SPACs

Pitchbook noted recently that "SPAC IPO activity exploded in 2021, with aggregate capital raised already surpassing the total in 2020 by 19.8% in just over one quarter." New SPACs ground to a halt in April as the SEC put down the regulatory damper, and capital markets struggled to find buyers for PIPEs. While there was a massive increase in the first quarter, pent-up demand is finally being realized.

While the pandemic put severe constraints on the process of identifying and making new investments, companies and investors got creative, relying heavily on virtual deal-making, which turned into high-resolution fundraising. But the massive spike in investment capital so far this year is probably not sustainable long-term. We might even call this a SPAC bubble, but since SPACs are useful tools, we'll probably see a moderation of demand over the year, rather than a sharp drop-off.

Monetizing Content

Nonfungible tokens (NFTs) are still growing in popularity, with people paying (seemingly) ridiculous prices for NFTs. After all, someone paid 300 ETH (roughly $590,000 at the time) for an NFT of Nyan Cat, a smiling animated cat with a Pop-Tart body, flying through space and leaving behind a rainbow trail. An NFT of a single tweet sold for $2.9 million. "Disaster girl" sold for $500,000. Some might notice some parallels to the 2017 initial coin offering (ICO) craze. Last month, I focused on how NFTs might find more widespread use for things like ticket sales and real estate, but the applications are much broader.

Brokerage company and cryptocurrency exchange eToro noted recently that "The aggregated market cap of the top 10 NFTs & Collectible Tokens has increased 764% YTD, climbing from $2B to $21B." Media mentions of NFTs have greatly surpassed those of DeFi, which was last year's hot crypto innovation.

Is the NFT market a bubble too? The sudden and explosive growth suggests that it is. But bubbles don't always pop in the same way. Finding a correct valuation is always difficult for a radically new market, and NFTs certainly qualify as a new market. They address a significant real-world problem for content creators: monetization. Consider the memes that I mentioned above. Meme makers are content creators, but until the advent of NFTs, they had no real way to profit from their work. NFTs are now offering meme makers the ability to profit from something that had typically been distributed for free and to do so in a way that doesn't hurt the free distribution of the meme. That last part is key. A meme's value depends on free distribution, and NFTs leave that intact while offering collectors the ability to have a provably limited version. Other kinds of content creators routinely struggle to make money from their work, but this new NFT market gives them a more direct way to monetize their content.

Emerging Automation Technology

One way to improve efficiency is to automate trivial tasks, and one method that has been gaining steam in recent years is using chatbots. A chatbot is a program designed to respond to users' questions and comments and provide meaningful guidance. Chatbots won't replace human staff for important conversations, but they can take over some of the mundane tasks that, while important, take staff time that could be better spent elsewhere. Time is money, after all.

Chatbots have been growing in popularity in a number of fields in recent years, finding their ways into industries like IT and construction. And while lawyers tend to be wary of new technology, chatbots are becoming more common in the legal field too. Chatbots are good at doing certain things, like helping potential clients find the right section of a website or schedule an appointment, the kinds of tasks that can be done by humans but don't need to be done by humans. Legal Tech noted last month that "where a chatbot can excel is assisting visitors with quickly navigating your website, routine questions or directions on how to schedule an appointment," not giving legal advice. Bots really can't replace lawyers. A lot of people think that technology will eliminate human work, but when we look at history, automation caused workers to shift into different jobs. While technology eliminated some jobs, it also enabled new jobs that had never existed before.

All of these technologies are part of the broad trend of digital transformation which we have been seeing in the past few years, and the pandemic has only accelerated the process. Today's trends seem to be pointing to continued investment in SPACs (after a correction), more direct connections between creators and consumers, and more shifting of mundane tasks to automation. The real world is becoming much more dependent on the virtual world, and while there are virtual bubbles in pockets, there is a virtual bull market.

United States: Artificial Intelligence Comparative Guide

Author: **Catherine Zhu | czhu@foley.com,**
Louis Lehot | llehot.foley.com

This article was originally published on Mondaq.com on April 21, 2021

Do you want to compare other jurisdictions?...
Click here

1 Legal and enforcement framework

1.1 In broad terms, which legislative and regulatory provisions govern AI in your jurisdiction?

Despite AI's ubiquity across every technology and healthcare field, there is no comprehensive federal legislation on AI in the United States to date.

The US Congress has nonetheless enacted and is considering several pieces of legislation that will regulate certain aspects of AI. The executive branch continues to adopt directives and rulemaking that will impact on the use of AI. In February 2020, the Electronic Privacy Information Center petitioned the Federal Trade Commission (FTC) to conduct rulemaking concerning the use of AI in commerce in order to define and prevent consumer harms resulting from AI products. We expect other organisations and groups to increasingly pressure the FTC and other governmental agencies to establish regulations regarding AI use.

Meanwhile, much of the governing legal framework is through the cross-application of rules and regulations governing traditional disciplines such as product liability, data privacy, intellectual property, discrimination and workplace rights. Self-regulation and standards groups also contribute to the governing framework.

1.2 How is established or 'background' law evolving to cover AI in your jurisdiction?

On the torts front, many states have passed autonomous vehicle (AV) legislation to help address liabilities associated with self-driving cars. For example, these laws may identify safety standards for AV testing, impose limits on AV manufacturers' liability or set insurance requirements.

At the federal level, following Executive Order 13859 and the establishment of the AI Initiative, the federal hub whitehouse.gov/ai was launched. Then, the Office of Management and Budget in early 2020 provided guidance regarding how to develop regulatory and non-regulatory approaches for AI technology and potential ways to reduce barriers to the use of AI to promote innovation in the private sector. The guidance provides for a set of principles (described in question 1.8) to consider when to formulate regulatory and non-regulatory approaches. The guidance further provides that if existing regulations are sufficient or if the costs of new regulation would outweigh the benefits, then relevant agencies may find alternative approaches. Some believe that the new AI guidance is or will become a de facto set of regulatory principles.

In April 2020, the FTC published further guidance regarding the commercial use of AI technology, acknowledging that while AI technology has significant positive potential, it also presents negative risks, such as the risk of unfair or discriminatory outcomes or the entrenchment of existing disparities.

The FTC urged companies to:

- be transparent with consumers;
- explain how algorithms make decisions;
- ensure that decisions are fair, robust, and empirically sound; and
- hold themselves accountable for compliance, ethics, fairness and non-discrimination.

Failure to uphold these principles could lead to liability for companies under the existing regulatory framework, such as:

- the Fair Credit Reporting Act,
- the Equal Credit Opportunity Act;
- Title VII of the Civil Rights Act of 1964;
- the Americans with Disabilities Act;
- the Age Discrimination in Employment Act;
- the Fair Housing Act;
- the Genetic Information and Nondiscrimination Act; and
- FTC Act general authority to bring enforcement actions regarding unfair and deceptive trade practices.

1.3 Is there a general duty in your jurisdiction to take reasonable care (like the tort of negligence in the United Kingdom) when using AI?

Yes, negligence is an established tort under US common law and is codified in many state statutes. The primary factors to consider for negligence are:

- whether an action lacks reasonable care;
- the foreseeable likelihood that such action would result in harm;
- the foreseeable severity of the harm; and
- any precautionary burdens to eliminate or reduce the harm.

Four elements that are required to establish negligence are:

- the existence of a legal duty;
- breach of that legal duty;
- sufferance of injury by the injured party; and
- proof that the defendant's breach of legal duty caused the injury.

1.4 For robots and other mobile AI, is the general law (eg, in the United Kingdom, the torts of nuisance and 'escape' and (statutory) strict liability for animals) applicable by analogy in your jurisdiction?

The United States applies tort liability for private nuisance and public nuisance. Another type of strict liability relevant to AI devices is consumer product liability, which relates to a manufacturer's liability regarding defective products.

1.5 Do any special regimes apply in specific areas?

Rights and protections for intellectual property are primarily regulated at the federal level, with some state-level statutes around trademarks and trade secrets.

1.6 Do any bilateral or multilateral instruments have relevance in the AI context?

The EU General Data Protection Regulation (GDPR) will likely affect AI companies that meet the establishment criteria for the European Union. Article 22 of the GDPR states that a "data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her", unless certain conditions are present. One permitted condition is based on express and informed consent by the data subject. This will likely affect how companies approach AI transparency and bias.

1.7 Which bodies are responsible for enforcing the applicable laws and regulations? What powers do they have?

No particular body is currently designated for enforcing AI-related policies. The enforcement of laws applicable to AI can be at the federal level, state level and/or private citizen level, depending on the area of law.

1.8 What is the general regulatory approach to AI in your jurisdiction?

No general regulatory framework on AI currently exists in the United States, but the White House Office of Science and Technology Policy has promulgated 10 principles to consider when formulating regulatory and non-regulatory approaches to the development and use of AI:

- Establish public trust in AI;
- Encourage public participation and public awareness of AI standards and technology;
- Apply high standards of scientific integrity and information quality to AI and AI decisions;
- Use transparent risk assessment and risk management approaches in a cross-disciplinary manner;
- Assess full societal costs, benefits, and other externalities in considering the development and deployment of AI;
- Pursue performance-based and flexible approaches so as to adapt to the rapidly changing nature of AI;
- Evaluate issues of fairness and non-discrimination in AI application;
- Determine appropriate levels of transparency and disclosure to increase public trust;
- Maintain controls to ensure confidentiality, integrity and availability of AI data such that the AI developed is safe and secure; and
- Encourage inter-agency coordination to help ensure the consistency and predictability of AI policies.

2 AI market

2.1 Which AI applications have become most embedded in your jurisdiction?

In the United States, AI exists in many different forms and through different functions and applications. Some examples of AI technology include:

- natural language processing;
- logical AI inferencing;
- machine learning;
- artificial neural networks; and
- machine perception and motion manipulation.

These technologies can perform functions such as automation, predictive analytics, image recognition and classification, speech-to-text and text-to-speech conversion, text analytics and generation, voice-controller assistance, and language translation.

Beyond specific technologies that are enabled by AI, market applications abound:

- In healthcare, AI allows users to analyse their own health data to identify anomalies, diagnose disorders and prescribe solutions;
- In the automotive realm, AI is facilitating the design and operation of autonomous vehicles (AVs);
- In finance and economics, AI is helping fund managers to deploy assets and harvest dividends and returns;
- In e-commerce, AI is assisting e-tailers in predicting which products consumers will want to buy and suggesting those products to them;
- In cybersecurity, AI is helping to identify and eliminate threats;
- In law, AI is being used to crunch terabytes of data in seconds and to identify discoverable evidence and conduct due diligence, identifying potential liabilities;
- In corporate governance, AI can assist in mitigating and managing risks, compliance and ethics within corporations;
- In video gaming, AI is being used to predict player behaviour, identify anti-social conduct and increase the sale of virtual goods; and
- In the military, AI is being used to identify threats and increase security.

2.2 What AI-based products and services are primarily offered?

AVs/systems, AI-enabled connected devices and software platforms using AI to provide services, are most common.

2.3 How are AI companies generally structured?

AI companies run the gamut from rapidly growing start-ups to large (even mega) cap companies such as Nvidia, Alphabet, Salesforce, Amazon and Microsoft. AI companies do not fall squarely within any traditional business model, as they often combine elements of a technology company, software company and services delivery model. Unlike software as a service companies, AI companies have continually high computing and data needs, as often a single AI model can require significant amounts of training data and computing resources. AI technology can also have demanding support and human oversight requirements, such as humans needed to manually clean and label datasets, or human input needed to augment AI-based systems. As AI companies begin to scale, we expect best practices and evolved business models to emerge.

Companies using AI can either develop AI capabilities themselves, license AI from a third party, acquire AI companies or a combination of the above. If developing AI capabilities themselves, companies should take pains early on to establish enforceable IP protection of their AI technology. If acquiring AI from a third party, a software licence will typically be required and the acquisition may also involve the purchase, lease or licensing of equipment, services or data. If exporting products to third countries, AI companies must obtain authorisations to export legally. The US government imposed additional export restrictions in January 2020 in an amendment to the Export Administration Regulations determined by the Department of Commerce, Defense and State. The measures were announced by the Bureau of Industry and Security and applied under the Export Control Reform Act of 2018. These restrictions make it harder for US companies to export AI technology, likely to help keep key technologies out of the hands of geopolitical rivals.

2.4 How are AI companies generally financed?

The United States has a highly evolved market for venture capital funds, based mainly in the San Francisco Bay Area, which pools capital and deploys it into private emerging growth companies in exchange for equity or debt instruments, providing differing levels of governance and economic rights. AI start-ups are typically financed by venture capital firms. For larger established companies that are evolving an existing set of products and services to integrate AI capabilities, these are funded by:

- research, development and innovation budgets;
- corporate venturing groups that secure the right to integrate such AI-enabled technologies from private emerging growth companies; or
- corporate development groups that acquire them on behalf of larger established companies.

Because of the proliferation of data, cloud and advanced computing capacities, there are lower barriers to entry for companies that are interested in entering the AI space.

2.5 To what extent is the state involved in the uptake and development of AI?

Most of the development of AI technology is happening in the commercial sector. However, the US federal government has provided guidance promoting and encouraging the development of AI technology; and certain federal agencies, such as the Department of Defense and others, are actively developing and promoting the use of AI technology. The Department of Defense has publicly expressed support regarding the importance of fostering innovation in the development and deployment of AI technology.

3 Sectoral perspectives

3.1 How is AI currently treated in the following sectors from a regulatory perspective in your jurisdiction and what specific legal issues are associated with each: (a) Healthcare; (b) Security and defence; (c) Autonomous vehicles; (d) Manufacturing; (e) Agriculture; (f) Professional services; (g) Public sector; and (h) Other?

(a) Healthcare

AI technology can be deployed in healthcare to gain information, process such information, and give a well-defined output, with the primary aim of analysing relationships between prevention or treatment techniques and patient outcomes. Hospitals and other healthcare providers may also deploy AI technology for operational purposes. Increasingly, insurance companies are seeking to leverage AI technologies to process claims and set policy prices. However, the use of AI in healthcare and insurance raises issues regarding algorithmic bias and other ethical concerns. Currently, there is no regulation specific to the use of AI in healthcare.

(b) Security and defence

The Department of Defense and other national security agencies are developing AI applications for a range of military functions. AI research is underway in the fields of intelligence collection and analysis, logistics, cyber operations, information operations, command and control, and semi-autonomous and autonomous vehicles (AVs). Competition exists at the global level regarding development of the 'best' AI technology. Some legal issues raised by military AI development include the risk of vulnerability and manipulation of AI technology, as well as ethical considerations.

(c) Autonomous vehicles

AVs are one of the primary areas where AI is applied, mostly through machine learning and deep learning. These vehicles are typically equipped with sensors, such as cameras, radars and lidar, to help them better understand and navigate their surroundings through the processing of large quantities of environmental input data. Some of the legal issues raised include the question of civil liability: if an AV injures someone in an accident, who should be responsible? The question of criminal culpability also arises: if someone falls asleep or is inebriated at the wheel in an AV, will that still be considered unlawful? Additionally, insurance law comes into question – specifically, whether the parameters of traditional auto insurance need to be altered, with new potential limits and exclusions.

(d) Manufacturing

AI technology can help manufacturers to digitise their factory operations. Some applications include:

- detecting defects throughout the production process;
- deploying predictive maintenance to reduce downtime;
- responding to real-time changes in demand across the supply chain;
- validating whether intricate goods have been produced to specifications;
- reducing the costs of small-batch or single-run goods to enable greater customisation; and
- improving employee satisfaction by relegating mundane tasks to machines.

Concerns regarding the replacement of human workers with AI technology, as well as ethical and labour implications, are rightly under consideration.

(e) Agriculture

Some of the more common applications of AI technology in agriculture include:

- the use of agricultural robots that can be programmed to handle essential agricultural tasks (eg, harvesting crops) at a higher volume and faster pace than human workers;
- the use of computer vision and deep-learning algorithms to process data captured by drones and/or other software-based technology to monitor crop and soil health; and
- the use of machine learning models to track and predict environmental impacts, such as weather change, on crop yields.

Regarding the use of AI robots and other AI-based equipment, legal considerations may apply regarding the operation of such machinery. States such as California are modifying their Occupational Safety and Health Administration regulations to impose new rules regarding the operation of AI-based machinery.

(f) Professional services

Professional services companies, including law firms, can use AI to help to automate a number of time-consuming or repetitive tasks, such as:

- reviewing and categorising a large portfolio of documents based on given criteria;
- extracting data from documents for analysis;
- identifying documents that are relevant for a request;
- maintaining consistency in document records; and
- conducting research and other tasks in support of compliance efforts.

(g) Public sector

The public sector has also been able to deploy AI technology, such as the use of chatbots to field incoming calls and questions from constituents, to free up time and resources for other functions. Other applications include using AI technology to:

- recognise and report objects in photographs and videos;
- translate dynamically between languages;
- monitor social media or public opinion for government-related topics or emergency situations;
- identify fraudulent activity or claims;
- automatically detect code violations;
- anticipate traffic flow and road maintenance needs; and
- measure the impact of public policies.

Just as with the use of AI technology in other sectors, AI technology in the public sector raises concerns regarding vulnerability to cyberattack and manipulation, as well as bias and discrimination in AI deployment and related ethical considerations.

(h) Other

AI technology is also being used in other sectors such as education, marketing, retail and e-commerce, as well as job recruiting and human resources.

4 Data protection and cybersecurity

4.1 What is the applicable data protection regime in your jurisdiction and what specific implications does this have for AI companies and applications?

The United States does not have a federal privacy law and instead currently has a sectoral model when it comes to privacy. Therefore, which privacy laws apply to an AI company will depend on the scope of its operations and the industry vertical in which it operates. For example, at the time of writing, a company will be subject to the California Consumer Privacy Act if it:

- makes more than $25 million in revenue annually;
- purchases or sells personal data annually of more than 50,000 California consumers, devices or households; or
- makes more than 50% of its annual revenue from selling California personal data.

Other states – such as Nevada, Illinois and Maine – have also enacted their own privacy laws. Similarly, if a company is in the healthcare space and is considered a covered entity, or in the fintech space and is considered a financial institution, then additional privacy regulations will apply. AI companies must determine which regulations are applicable to their business. In some cases, AI companies may be subject to certain restrictions when it comes to automated decision making. They may also need to:

- procure necessary consents;
- impose purpose limitations or data minimisation;
- provide notices; and/or
- meet other data privacy requirements.

4.2 What is the applicable cybersecurity regime in your jurisdiction and what specific implications does this have for AI companies and applications?

There is no regulatory cybersecurity regime in the United States; rather, applicable privacy laws for the most part defer to (and require implementation of) accepted industry standards when it comes to cybersecurity.

5 Competition

5.1 What specific challenges or concerns does the development and uptake of AI present from a competition perspective? How are these being addressed?

Businesses may use AI to respond more quickly to changing market conditions, innovate their products, set pricing and take other actions that can have antitrust considerations. While there are clear commercial benefits to being able to respond rapidly to market conditions and re-set pricing in real time, this can be used in an anti-competitive manner, such as by engaging in collusion with competitors or reaching other anti-competitive agreements using AI systems. In some cases, the AI system may be able to develop sufficient learning capability to arrive at an anti-competitive conclusion (eg, that collusion with a competing AI system is the optimal action to take), independent of any human direction or decision. This is still a developing area of law, but we expect regulators to seek to hold companies responsible for the actions of their AI, and to want companies to build compliance measures into their AI from the outset.

6 Employment

6.1 What specific challenges or concerns does the development and uptake of AI present from an employment perspective? How are these being addressed?

One specific challenge, as autonomous vehicles are developed, is whether employers will expect or require employees to check work email or perform other tasks while 'driving'. This may then lead to other considerations, regarding wages and other workers' compensation issues. There is no current regulation on this particular concern; such regulation will need to be promulgated as the technology develops,

Another general challenge of using AI technology for employment recruitment and hiring purposes is the issue of discrimination. Concerns include:

- disparate treatment, where there is intentional discrimination against individuals of a protected class; and
- disparate impact, where facially neutral practices disproportionately impact on members of a protected class.

Privacy concerns also exist as they relate to background screening of potential employees. A number of federal laws prohibit workplace discrimination, such as Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act and others. State anti-discrimination laws are similar to the federal laws, but may offer additional protections against employment-related discrimination.

7 Data manipulation and integrity

7.1 What specific challenges or concerns does the development and uptake of AI present with regard to data manipulation and integrity? How are they being addressed?

Data manipulation and integrity is a significant concern, as the use of AI technology proliferates. Failure to maintain the integrity and security of AI systems may lead to a lack of public trust, which would hamper the adoption and development of AI technology. Some specific concerns regarding AI technology include:

- vulnerabilities and blind spots in sensor technology and neural networks;
- manipulation of visual data to trick deep learning systems;
- backdoors and triggers which can be maliciously trained into algorithms by outsourced third parties; and
- misappropriation of AI systems by hackers.

While it is possible (and likely) to impose legal liability in the wake of these negative events, preventative approaches should be employed with regard to data manipulation and integrity.

8 AI best practice

8.1 There is currently a surfeit of 'best practice' guidance on AI at the national and international level. As a practical matter, are there one or more particular AI best practice approaches that are widely adopted in your jurisdiction? If so, what are they?

At a high level, AI best practices should help to address concerns and seek to improve the quality, integrity and accuracy of the AI system. Google, a leader in the AI technology space, has recommended the following best practices:

Use a human-centred design approach with a focus on the user experience, which should encompass a diversity of users and use cases;

- Identify multiple metrics to assess training and monitoring, where such metrics should be appropriate for the context and goals of your system;
- Where possible, directly examine your raw data to assess accuracy and predictive capabilities;
- Understand the limits of your dataset and model, and communicate these limitations where possible;
- Conduct rigorous, diverse and regular testing of your AI system; and
- Continue to monitor and update the AI system after deployment to take into account real-world performance and user feedback.

8.2 What are the top seven things that well-crafted AI best practices should address in your jurisdiction?

See question 8.1.

8.3 As AI becomes ubiquitous, what are your top tips to ensure that AI best practice is practical, manageable, proportionate and followed in the organisation?

As with the implementation and deployment of any other internal process, identifying and communicating clear objectives and actionable steps to accomplish those objectives across all levels of the organisation, including in relation to functional groups, will be necessary. It would also be helpful to document processes and responsibilities, as well as learnings, to the extent possible. Separately, building a culture that encourages and values the development of AI in a thoughtful, ethical manner, and that understands the potential dire consequences of failure to do, so is also important.

9 Other legal issues

9.1 What risks does the use of AI present from a contractual perspective? How can these be mitigated?

Companies that license or purchase AI technology for incorporation into mission-critical functions should carefully consider the AI vendor's risk allocation from a contractual perspective. Any AI system failure or equipment malfunction can have catastrophic consequences. The vendor's representations and warranties and associated liability regarding the AI system's performance and output should adequately address the potential business impact and damages in the event of a system failure. For any physical AI equipment, the vendor's representations and warranties and associated liability should cover injuries and other damages caused by such equipment. The vendor's liability in these instances of system or equipment failure should encompass third-party claims, as such situations will affect downstream users and may cause significant reputational damage to the company.

9.2 What risks does the use of AI present from a liability perspective? How can these be mitigated?

See question 9.1. Another mitigation mechanism to consider is insurance. The vendor and the customer can limit their liability exposure by shifting some risk to an insurer. This can be covered through commercial general liability insurance, cyber insurance, errors and omissions coverage, business interruption coverage, and other types of insurance applicable to the ways in which AI systems can fail or cause damages.

9.3 What risks does the use of AI present with regard to potential bias and discrimination? How can these be mitigated?

Because AI is trained largely on real-world datasets, it can integrate and deploy existing biases. For example, a criminal justice algorithm used in law enforcement may incorrectly identify black individuals as 'high risk' at a higher rate than white individuals. Algorithms may also integrate gender expectations and stereotypes. For example, a hiring algorithm may favour applicants based on action verbs used more commonly by men than women, leading to a disparate impact. Groups who are underrepresented in training data may result in a higher error rate of the AI technology regarding underrepresented groups in deployment.

To mitigate these potential biases and discrimination, it is important to be cognisant of the presence of bias and to develop criteria for measuring bias in AI technology. Doing so will require a multi-disciplinary approach, including a technical solution, as well as perspectives from ethicists, social scientists and others.

10 Innovation

10.1 How is innovation in the AI space protected in your jurisdiction?

Innovation in AI, like other technologies, is largely protected through IP law. Intellectual property in the United States is primarily protected through patents, trademarks, copyrights and trade secrets. As it relates to AI, certain forms of AI are patentable, which is expressly recognised by the US Patent and Trademark Office as a Class 706 designation. Copyright protection is also available to certain types of AI, such as source code and visual elements of an AI computer program. However, datasets and algorithms, which are both key elements of AI technology, may not fall under copyrights or patents as registrable intellectual property; consequently, trade secret protection can also be useful for AI. Trade secrets are protected at the federal level in the United States, as well as at the state level through state trade secret statutes. Trade secret protection can offer advantages over patents or copyrights as a form of intellectual property, because it can last indefinitely and there is no application or registration process. Instead, the trade secret owner must make significant and diligent efforts to obtain and maintain trade secrets compared to other forms of IP protection.

10.2 How is innovation in the AI space incentivised in your jurisdiction?

Because of the numerous potential applications and commercial uses of AI across a myriad of industries, there are significant profit and market incentives for AI companies. Additionally, at the national level, the United States is interested in encouraging and fostering AI innovation to remain globally competitive. As AI technology continues to develop, we will likely see policies and regulations emerge to foster and reward innovation, such as consumer tax credits for the adoption of AI technology. We may also see:

- sector-specific policy guidelines or frameworks to encourage AI innovation;
- the granting of exemptions or allowance of pilot programmes that provide safe harbours for specific AI applications; and
- voluntary consensus standards for AI applications.

11 Talent acquisition

11.1 What is the applicable employment regime in your jurisdiction and what specific implications does this have for AI companies?

Talent acquisition and retention is an increasing area of application for AI technologies, which seek to automate recruiting and hiring, employee onboarding and management of human capital. Facial recognition applications of AI, among others, could have significant impacts on an individual's ability to obtain and retain employment. The risk of discrimination attracts attention, as well as the ethical concerns implicated by the potential disparate treatment or disparate impact of AI on certain pools of talent. Employers using AI tools must also ensure that they do not violate privacy rights that are codified in federal password privacy laws, salary history bans and biometric privacy laws.

In the United States, employment is governed on a state-by-state basis, with an overlay of federal laws to prohibit discrimination, harassment and retaliation based on gender, race, creed or identification with another protected class. While there has not yet been a federal statute adopted on AI in the workplace, the US Congress is considering a law that would create a moratorium on the government's use of facial recognition technology until a commission recommends the appropriate guidelines and limitation for its use.

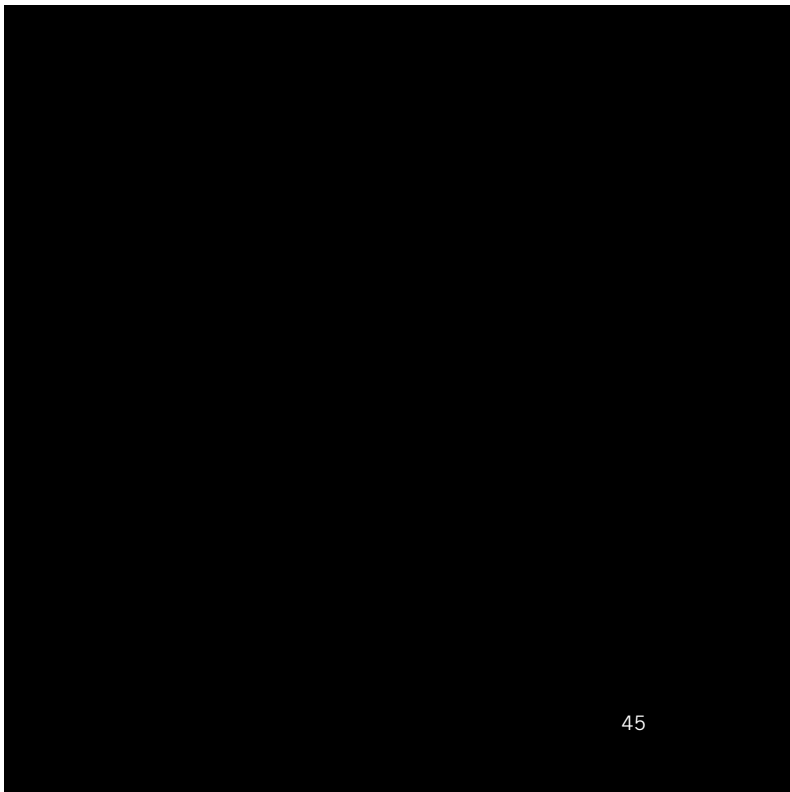
11.2 How can AI companies attract specialist talent from overseas where necessary?

The employment of non-US-born computer scientists, programmers and engineers to create AI technologies and form AI companies is a subject of great controversy in the United States. While historically, the US immigration laws were applied by the executive branch to recruit and retain specialist talent from overseas, this has become a subject of increasing controversy in recent years, with the 45th president, Donald J Trump, passing directives aimed at curbing the flow of immigrants, even those with special skills. Moreover, the US Congress passed legislation (supported and signed by Trump, implementing the legislation into binding statute) to reinforce the powers of the Committee on Foreign Investment in the United States, to ensure that AI technologies are not exported by the United States to third countries, particularly China, and has placed significant controls on investment in companies developing AI technologies.

12 Trends and predictions

12.1 How would you describe the current AI landscape and prevailing trends in your jurisdiction? Are any new developments anticipated in the next 12 months, including any proposed legislative reforms?

The legal and regulatory framework is working to catch up with the pace of technology when it comes to AI. Governments at the federal and state level are exploring potential regulatory and non-regulatory approaches to overseeing AI without stifling innovation. We may start to see more regulations, such as ones that have been enacted at the state level for autonomous vehicles, while keeping in mind the goal of finding the right balance between protecting consumers and the general public and simultaneously stimulating innovation in AI.



13 Tips and traps

13.1 What are your top tips for AI companies seeking to enter your jurisdiction and what potential sticking points would you highlight?

For any AI company, the AI technology or product should solve a problem with sufficient market potential in order to be successful. AI development can be resource-intensive, so the company must assess whether it has enough runway and market potential to sustain itself. Building AI will involve continual testing and improvement of the company's AI technology. Separately, it is also important to be able to execute on multiple fronts as a business beyond the development itself. For example, companies will need to engage in PR/external communications to raise awareness of their products; they will also need to develop revenue-generating channels with potential customers and partners.

As the use of AI technologies becomes ubiquitous, those companies that can solve specialised problems unique to specific industry verticals will differentiate themselves from the pack. Research indicates that vertically specialised AI companies have a higher potential for fundraising and exit, even if exit valuations are lower than horizontal AI companies that finally succeed in exiting.

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

The State of the Acqui-Hire in 2021: The good, the bad, the why and what's next

Acqui-hiring refers to a merger, acquisition, or asset purchase.

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on TealFeed, May 2021

In the technology industry, whether in Cupertino or elsewhere in the Global Silicon Valley, the competition for the top talent required to grow to scale can be fierce. For decades, there have not been nearly enough STEM graduates to fill open spots.

The road from #garage2global is tortuous, and a key ingredient to becoming #bigtech faster than the next #startup is hiring engineers. For #bigtech companies to stay on the cutting edge, they often find that acqui-hiring a startup with ten engineers is a faster, better return on investment than hiring onesies on a drip-feed basis.

What is an acqui-hire?

Acqui-hiring refers to a merger, acquisition, or asset purchase whereby the buyer seeks to secure the target's talent, engineers and personnel, rather than to develop or monetize the target's technology, products, or services. It can be a very efficient way to grab talent in groups.

When a #bigtech company acquires a group of highly-skilled engineers who have a strong working relationship, they can hit the ground running seamlessly and with gusto, which benefits all. Especially the bottom line.

This "recruitment" process can cut costs and potentially prevent possible legal action relating to non-compete clauses, I.P. infringements, and breach of contract. An acqui-hire can also be tidier than a failing company's wind-down process but often signals a distressed sale.

Many of these companies could not get additional funding needed to continue, and often, the entity acquired is shuttered post-closing.

History of acqui-hires — a threat to the competition?

The tech sector phenomenon of acqui-hires is not new: Google has made 200 acquisitions since being founded in 1998 by Sergey Brin and Larry Page, the vast majority of which have been acqui-hires. Facebook has acquired more than 80 companies.

In a 2018 interview with CNBC, Tim Cook, CEO of Apple, bragged that Apple acquires a company every 2 or 3 weeks, either for talent or intellectual property. Amazon has acquired over a hundred companies, and Microsoft many multiples of this number.

Early in 2020, the Federal Trade Commission made public a probe into possible market abuse by #bigtech by demanding information on all acquisitions not already reported to antitrust authorities in the past decade.

While investments over a statutory threshold are reported in a government filing before closing, acqui-hires are typically for amounts well below the threshold and have flown under the government's radar.

In its special orders issued to the big five #bigtech companies — Amazon, Apple, Facebook, Google, and Microsoft — the government asked for details on terms, scope, structure, and purpose of each transaction consummated between January 1, 2010, and December 31, 2019.

Within the purview of the orders was a wide variety of transactions, no matter how structured, from minority investments to licensing deals to board designation rights.

By December 2020, the FTC had sued Facebook, alleging that the company had "illegally maintain[ed] its social networking monopoly through a year-long course of anticompetitive conduct." The lawsuit was joined by the elected attorneys general of 46 states, the District of Columbia and Guam. The complaint alleges, notably, that Facebook used acquisitions as part of a systemic strategy to eliminate threats.

Structures and value

Structures can vary, but typically it's an acquisition of stock or assets, with the bulk of the purchase price being held for employee packages.

If the buyer only wants the team, they may sign a release agreement where the company agrees to release the buyer for hiring the employees and include a defensive license agreement of the company's I.P.

When it comes to pricing, buyers frequently express the price on a "per head" basis, and the rate can be a few hundred thousand or two million dollars per head.

There are no set rules for an acqui-hire, which are often a combination of stocks or assets. These agreements are often light on terms since the real value is the employees, not the company, and to do an acqui-hire successfully, the buyer must get the team to agree to join the new company.

An annual contract is standard, and sometimes, the employee is enticed to join with a signing bonus. However, there is a risk they leave the moment the contract is up and use their experience to begin another company.

For buyers considering an acqui-hire, consider:

- Will there be post-merger liabilities?
- How will obligations to creditors be satisfied?
- What structure will the new employee's compensation take?
- Have you completed a rigorous due diligence process, ensuring you and your stockholders are getting value for money?
- Have you considered the liabilities of terminating existing employees?
- Have you thought about a deal structuring where the company, not just the people or assets, are acquired, avoiding a separate wind-down process?
- Have you consulted with tax advisors early in the process on complicated tax questions, such as parachute payment tax considerations

Buyer keys to success

The keys to the success of an acqui-hire typically can be traced back to three key drivers:

- Retention. To obtain a positive return on investment, a buyer needs a target talent to remain with the buyer. Structuring payments to target talent over time can motivate teams to stay in their seats and achieve results. Should payments be linked to the passage of time, the achievement of milestones, or have some incentives for each?
- Non-competes. While California and some other jurisdictions have rendered illegal the use of non-competition and other restrictive covenants, the exception is for covenants given in the context of the sale of a company's business. They are usually less scrutinized when made in connection with an acqui-hire. Nevertheless, they need to be carefully drafted to be enforceable. In addition to non-competes, there can be non-solicits, no-hires, confidentiality, and invention assignment agreements.

- Personalization. When buyers spend enough time with targets and their teams, they can identify some key ingredients to their success. The deal should be personalized to the circumstances of each target. Employment agreements, offer letters, equity awards, and other deal elements should not merely be standard forms rolled out of the buyer's H.R. department, but rather, narrowly tailored to capture the target's value
- Paying attention to these key deal drivers will often be outcome determinative as to ultimate success.

Buyer benefits

With the completion of an acquihire, a company may now be better able to develop new technology, enter a new market, or support an existing technology function or market position thanks to the recent influx of talent. The new hires may bring with them new ideas and processes.

An acqui-hire can inject new blood into an engineering team that has become bureaucratic, bringing innovation, new ways of doing things, new products, or improving existing products.

Drawbacks

The negative aspects of an acqui-hire are not always apparent. Distance between buyer and seller offices and the question of where the seller's team will sit post-closing can be disruptive. Additionally, working for a larger company comes with different rules that are more restrictive than most startup environments.

For the buyer, what if the target's talent does not join or departs shortly after? Hopefully, the buyer has smartly crafted a deal where the target's talent feels incented to stick around and make things happen.

Another hidden danger of an acqui-hire for the buyer is the morale of current workers. Bringing in a new team from the target can cause resentment among the buyer's existing workforce, especially if the target's team parachutes into the buyer's team with elevated positions.

Why sell in an acqui-hire?

So, if you are a startup looking at an acqui-hire term sheet, what to do? Let's face it: most startups will fail with the first two to five years of their existence. A startup is a gamble in the best of circumstances. What if you can't build the product?

What if the market isn't there? What if you can't raise the funds that will be required for startup capital? What if someone comes in and does it faster, better, cheaper? What if you can't raise scaling capital? The unexpected is always expected. For the seller, an acqui-hire on the right terms can be the safest crash landing, or it can be a home run.

Outlook for 2021

While the global pandemic has been lethal to the hospitality and travel sectors, it has not been catastrophic to the technology industry. The stock market is at record highs. A new administration is arriving in Washington.

A natural question is whether we can expect the acqui-hire to survive and thrive in 2021. While the acquisition programs at the five #bigtech companies under FTC investigation can be expected to slow down, there is no reason to think that the rest of the technology industry won't carry on with this tried and true growth driver.

Quantum computing advantage: Today and tomorrow

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on Global Trade Magazine, January 21, 2021

To date, the power of computing has enabled a remote economy, remote healthcare, remote collaboration, remote education, secure and contactless transactions, and intelligence that surpasses the human mind. New quantum computing power will usher in a brand new era — providing massive rewards to the companies and countries leading in the space, leaving laggards in the dustbin of history.

Paving a New Road Ahead

We didn't need MIT to name quantum computing a breakout technology back in 2017 and again in 2020 to know quantum computing is paving a new road ahead. Recently, Google solved a problem in just over three minutes with a quantum computer that would have taken a supercomputer longer than 10,000 years to solve. While excellent news, not many understand what a quantum computer does, and many investors don't know what quantum computing means for their portfolio. Still, the quantum computing opportunity has never been more relevant than it is today.

In the last few years, quantum computing has been making traction, with many companies building systems that aren't powerful enough for most real-world use cases yet, but still, show promise. Tomer Diari, an investor from Bessemer Venture Partners, told TechCrunch, "Quantum computing will drive a paradigm shift in high-performance computers as we continue pushing the boundaries of science deeper into the realms of science fiction."

The Leader in New Tech

In last year alone, several breakthroughs from research, venture-backed companies, and the tech industry have unlocked the challenges in scientific discovery. This has moved quantum computing from science fiction to reality and armed it to solve significant world problems.

Companies like Atom Computing leveraging neutral atoms for wireless qubit control, Honeywell's trapped ions approach, and Google's superconducting metals, have all seen first-time results, setting the stage for the first commercial generation of quantum computers.

At just 40-80 error-corrected qubit range, these systems could deliver capabilities that surpass classical computers, which will, in turn, speed up the ability to perform better in areas like thermodynamic predictions, chemical reactions, resource optimizations, and financial predictions. Companies like Microsoft, IBM, and Intel, and Google are further ahead than anyone else has been to unlock the quantum computing scope. As many technologies and ecosystem breakthroughs begin to converge, the next year will be a decisive moment.

Investors Are Spending

Recently, Quantum computing startup Rigetti Computing raised US$79 million in a Series C funding round, which was led by Bessemer Venture Partners and intended to advance its efforts in making quantum computing commercially viable, according to Business Times. EDBI, Singapore's Economic Development Board, Franklin Templeton, Alumni Ventures Group, DCVC, Morpheus Ventures, and Northgate Capital, also participated in the round.

"This round of financing brings us one step closer to delivering quantum advantage to the market," said Chad Rigetti, founder and CEO of Rigetti, a company that builds and delivers integrated quantum systems over the cloud and develops software solutions optimized for hybrid quantum-classical computing. Hybrid models like this one leverage quantum and classical computations – a more practical quantum computing approach.

Controversy

In a piece published in Science, researchers in China used quantum mechanics to perform computations in minutes. This would have taken billions of years using conventional machines. The research, which used photonic quantum computers, shows what claims to be the very first definitive demonstration using a "quantum advantage" to solving a problem that would have been impossible with classical computers.

However, as mentioned above, last year, Google built a quantum computer that they said achieved "quantum supremacy" and performed computations in minutes that would have taken the most powerful supercomputers tens of thousands of years. Google's quantum computer was programmable. Google's claim has been contested throughout the quantum computing field and many argued that a classical supercomputer could have performed the computations faster with a better algorithm. This back-and-forth and the fact that the area can't agree on whether to call these achievements "quantum advantage" or "quantum supremacy" shows quantum computing is still a developing technology.

Looking Ahead

A quantum computer comprises qubits that can store an infinite number of values while still providing a single measure. Still, a regular computer can only store one value in one register, according to Forbes. Like A.I., the quantum world is entirely built on probabilities, which has led us to be engulfed in fascination with the possibilities and chances on the horizon. Both the hardware and algorithms have a long way to go until they grace our level of environments. It's not an unattainable innovation, though – it's reachable enough to learn and research for now.

Recent signs show that the lab's progress is starting to transfer into commercial products, specifically in cloud computing. Xanadu announced a partnership with AWS to bring its open-source quantum software library PennyLane to the cloud computing giant. Additionally, IBM reached one of the most accepted general quantum computing performance measures on one of its systems.

A brief legal guide to buying and selling shares of private company stock

Author: **Louis Lehot | llehot.foley.com, Natasha Allen | nallen@foley.com,**
Brandee L. Diamond | bdiamond@foley.com, Catherine Zhu | czhu@foley.com

This article was originally published on Foley.com on March 29, 2021.

What to expect in a secondary market transaction

You formed and financed an emerging growth company or startup, you hold unregistered shares of a private company not listed on a national securities exchange—but you need cash now.

You run a company or sit on a board of directors of a private company where a stakeholder has notified you of its intent to obtain liquidity for a stake of shares.

What are your choices?

If you are still with the company, what signal is sent by your desire to sell? If you are the company, what signal is sent by your facilitating a secondary transaction? Are you promoting or detracting from retention? Are you helping or hurting your company's ability to raise capital in the future? What do you need to know to navigate the murky waters of the secondary markets as a buyer or a seller?

Historically, a private company stockholder would have to wait until the company goes public or gets acquired to get a return on investment of sweat equity or of early capital. But as the path from ideation to public listing has been extended this century, so has the pressure to obtain or enable a liquidity transaction.

Stockholders in many private companies are increasingly participating in "liquidity rounds," also known as secondary sales, where they sell shares of stock for cash before the company goes public. There are many factors that a holder or a private company should consider when deciding if and how to structure this type of transaction. Will a liquidity transaction help a company retain key talent, or is it enabling its own demise by helping its key talent achieve an early exit? Is it fair to those that are participating and those that are not given access? There are also specific steps a company can take to control secondary transactions in its stock in the future.

The following is a brief legal guide to key considerations in buying and selling shares of private company stock in liquidity rounds.

Liquidity transactions can be structured as a buyback of shares by the company—funded by balance sheet cash or cash from an equity financing. Alternatively, the transaction might be structured as a direct purchase of shares by a third party, pairing the purchase with a company's primary equity financing or even as a standalone transaction. In a company-sponsored transaction, the company must decide the limits and the stockholders that can sell shares.

Just like with any securities transaction, it's wise to consult with the company's legal and tax advisors to be sure that all required approvals are received, determine the appropriate tax, reporting, and withholding requirements, and prepare the right documentation. Other important legal considerations must be taken into account, including what disclosures are made by the seller to the buyer, and who knows what at that time. Will the information about the issuer leak to competitors or cause damage if learned by customers? These concerns can be accentuated in a tender offer by a company or a third party to holders. What will be said in a future S-1 filing about the transaction? How will the transaction impact a company's prior or subsequent determination of the fair market value of its common

stock for purposes of making future equity grants (e.g., the "409A value")? What capital gains will be reported? How will such a transaction impact the federal tax-free status of the shares under Section 1202 of the Internal Revenue Code, commonly referred to as "QSBS rules?"

As with any transaction involving stock, the parties may have liability for disclosing relevant material and nonpublic information to the other parties (or for failing to make the disclosures!). This is critically important when the sellers do not have board-level details about the company. Whether the company has liability exposure will depend on its involvement and the relevance of any undisclosed information. Making disclosures to potential buyers can trigger leaks to competitors, customers, suppliers, or other ecosystem players that could be dangerous to the issuer of the stock.

When secondary purchases are made via a "tender offer," depending on the number of sellers, the transaction may need to be structured to comply with certain components of the SEC's Regulation 14E.

Moreover, transactions occurring between the company, its officers, and others within the three years prior to the IPO must be disclosed as related-party transactions in the company's IPO filing on Form S-1. A third-party purchase not involving the company could be required to be disclosed depending on its materiality. Some states, including Delaware and California, have statutory balance sheet tests limiting the amount of capital that a company can use to buy its shares.

The degree to which any transaction will impact the company's 409A valuation depends on the terms of the transaction, the parties' identities, the transaction size, and the valuation firm's methods.

A purchase of shares priced above what the company's board of directors otherwise considers "fair market value" of the common stock creates the risk that current or former employees or service providers selling shares won't be able to claim capital gains treatment on 100 percent of the sale price. So, the difference may need to be taxed as regular income, and then the company may have a withholding obligation.

A company's buyback of shares may impact whether or not the shares held by other stockholders qualify as QSBS for federal income tax. A third-party purchase will not have this impact, but the shares purchased won't be eligible as QSBS. Therefore, consideration should be given to whether or not the transaction requires a "Hart-Scott-Rodino" antitrust filing, which involves much effort and a hefty fee.

How do you ensure your company has control over secondary transactions in shares in the future? It would help if you considered implementing a "right of first refusal" over your company's stock transfers. Common stock can be subject to a right of first refusal, which provides the opportunity to purchase shares that a stockholder proposes to sell to a third party. The right of first refusal is usually contained in the company's bylaws, so it automatically applies to all shares issued after the bylaws are adopted. This is a useful way to control stock ownership to the extent that the company or its assignee can spend the necessary funds to purchase the shares. If not, the shares can be sold to the proposed buyer.

A private company tends to feel pressure to provide liquidity to its stockholders as its value increases. So, whether you decide to engage in a liquidity transaction or permit your stockholders to sell while the company is private, setting your stockholder expectations both early and clearly can go far. Getting the details right will save you legal, accounting, HR, and tax headaches that are imminently avoidable.

Five market, investment, and M&A trends in Medtech meet five legal and policy issues

Medtech businesses show tremendous potential for profitability and growth, triggering a sparked interest in investment.

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on MedTech Intelligence on March 11, 2021

Accelerated by the response to the global coronavirus pandemic, technology has radically prompted healthcare disruption in fundamental ways. Technology is drastically changing how healthcare is delivered to patients and creating new business models for innovative organizations. Never has the medical technology industry been so attractive to investors. Medtech businesses show outsized potential for profitability, resiliency, and growth, fueling an investment bonanza from private equity investors.

Market Characteristics

Size. With total annual revenue of $510 billion in 2019, the medtech industry is increasing its share of the whole healthcare pie. We look at this industry as forming five primary areas: Medical equipment, medical devices, medical consumables, in-vitro diagnostics, and life science tools. With success also come challenges. Pre-COVID, the medtech industry faced pricing pressure, maturing products, and increased pressure to show differentiation. Investors looking at these businesses would be wise to evaluate forecasted growth in the face of these potential headwinds.

Components. While we primarily view medtech around the five areas as mentioned above, it nonetheless remains highly fragmented. For PE investors, fragmentation is attractive, as it offers the possibility to buy and combine multiple companies and achieve revenue growth and cost synergies. Together, the 10 largest medtech companies have only about 40% of the market, and no single company generates more than 8% of revenue. Meanwhile, large organizations can create value through scaling. Therefore, the biggest companies in the industry are looking to get bigger. This is achieved through M&A initiatives to generate scale efficiencies, acquire R&D, and access growth segments. In addition to the large companies, the industry also has many small and midsize companies that can provide value in different segments, regions, and specialties.

Demographics. Demographic trends such as the aging first world population and increasing chronic lifestyle illnesses like diabetes translate to greater demand for medtech products. Emerging markets where access to care is growing can offer a significant source of growth.

Change. Healthcare and healthcare services are also changing dramatically. Treatments are moving from traditional settings like doctors' offices and into patient homes, with consumers paying a more prominent role in their care. This change is increasing the opportunity to create new markets, as technology enables new business models with the potential to create growth.

Procurement. Today, the procurement function is centralized at a high level, so medtech companies need to offer more significant discounts to gain a smaller number of large accounts. Rather than primarily selling products per-unit, innovative companies develop solutions to create value in the patient journey.

Investment Trends

Four core investment trends in 2021 will support increased value creation in the medtech industry, including innovation, patient journey, consumerization, and efficiency. These can offer investors a more strategic way to think about the opportunities in the marketplace.

Innovative Technologies. The technology available allows companies to develop unique products that are cheaper to create and more efficient to operate. For example, 3-D printing technology can develop robotic surgery infrastructure or investigate products to address unmet needs in certain areas. Medtech is the innovative solution to the problem.

Evolving Product Models. Moving far past its traditional role, healthcare is creating opportunities for medtech companies to develop new product models. For example, a company can sell its clinical products to both physicians and healthcare facilities, as well as directly to patients. These types of new product offerings are pushing many medtech companies to evolve beyond traditional transactions.

Consumers in Control. Consumers are getting more individual control over their care. For example, diabetes patients have always needed to monitor their insulin levels, and new technologies are emerging to give them better tools that make it easier. Many companies offer mobile apps to help patients by sending data securely to doctors and sending alerts in situations requiring more support.

Operational Optimization. The industry has historically had high-profit margins, but it has needed to become more operationally efficient as of late. Medtech has a much higher cost structure than other sectors, which shows there is area for improved optimization. For instance, to increase efficiency, some companies could benefit simply from outsourcing production, while others could improve procurement by consolidating their supplier network.

M&A Activity

According to a recent E.Y. report, the dearth of medtech deals in 2020 combined with the huge pile up in cash reserves among leading strategic players and interest from PE shows promise for a healthy 2021. While in 2020, non-emergency procedures were deferred, a backlog of activity should power a growing quarter over quarter and year over year performance base for medtech businesses. With the IPO window wide open and a frothy stock market, mainly driven by special purpose acquisition corps, or SPACs, growing medtech businesses have prospects for dual-track exit processes.

We think medtech is ripe for significantly increased M&A and investment activity and deal flow in 2021. By understanding the dynamics shaping the industry and applying the relevant trends, entrepreneurs should be navigating towards successful liquidity events, and investors can ensure success.

Legal and Policy Issues

The global pandemic response brought renewed urgency to policy issues facing medtech businesses in 2020 and should hasten legislative and regulatory responses in 2021.

Infrastructure. Our healthcare system's fragmented nature in the United States serves as a block to healthcare delivery, while the decentralized payor system and comprehensive technology solutions offer new solutions. We expect new initiatives to strengthen infrastructure and support diagnostic testing, vaccination, and healthcare delivery. While these efforts will initially be designed to respond to COVID-19, these same initiatives should remain in place to deliver any healthcare service, which could be a massive opportunity for medtech businesses.

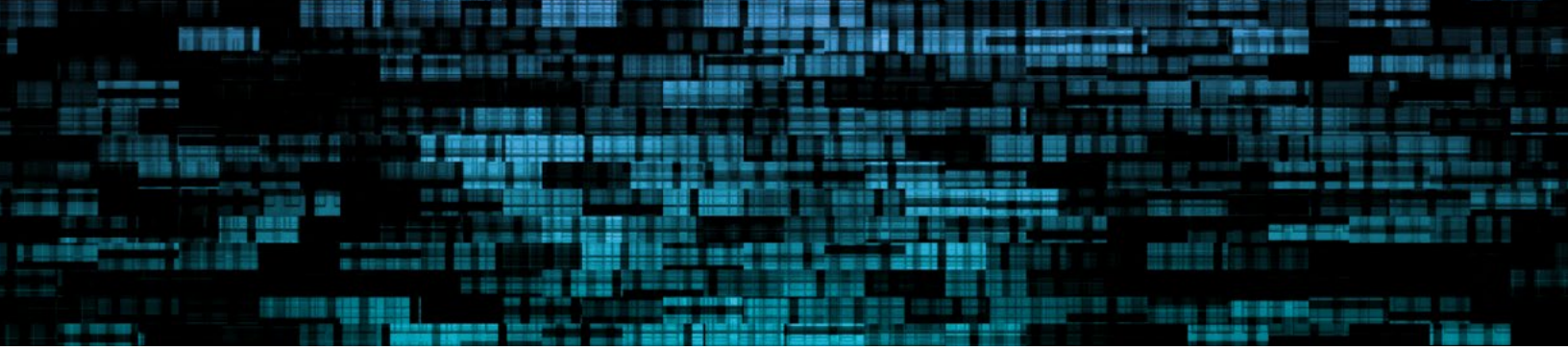
Access. In the United States, the disproportionately negative impact suffered by the minority, immigrant, and lower-income communities highlights the problem of access to healthcare for all. With waves of pandemic contamination impacting regions and populations, healthcare access becomes critical to contain the spread and maintain economic output. We expect that federal, state, county, and city initiatives to allocate capital to increase access, initially through telehealth services, will augment access for all.

Clinical trials. As the COVID-19 coronavirus mutates and new strains have different responses to approved vaccines, clinical trials will be necessary for both vaccines and treatments. The decentralized nature of the U.S. healthcare system will need to allow for decentralized clinical trials, in multiple languages, in different media, and serving diverse populations.

Diversity. The age of personalized medicine continues, and technology solutions from medtech businesses that have outsized returns will be targeted to patient populations. Policy initiatives to extend access to services will be made to diverse populations, both inside and outside the country. Medtech businesses will need to plan for diversity in the product roadmap.

Privacy. The coordinated response to the coronavirus pandemic has brought an unprecedented incursion into personal privacy. Many commercial establishments require entrants to fill a form that asks for personal data—and this data is collected, stored, and transmitted to enable contact tracing. Will proof of diagnostic testing and vaccination become a matter of public record? Will it be a condition to accessing essential services we consider fundamental to human rights? Where is the line?

The global pandemic has drastically changed the healthcare world in so many life varying ways. Overall, we think medtech businesses that design the right legal and policy solutions into their roadmap will benefit from more significant investment and outsized economic returns. With new and innovative technology disrupting and improving how healthcare is delivered to patients, healthcare will never be the same. It is truly making the world a better place for patients and providers alike. Therefore, the medtech industry has never been so attractive to investors.



Considering selling your company? Be clear on your fiduciary duties

Looking out for everyone sometimes means going the extra mile.

Author: **Louis Lehot** | **llehot.foley.com**

This article was originally published on Medium.com on February 18 2021

These days, most entrepreneurs bring their companies to market for sale for one of three main reasons:

1. It was a goal from the start to launch a business and sell it eventually;
2. The venture has not been making any significant progress since its inception or;
3. It is time to leave the business industry and enjoy retirement with the profits acquired. More about the eight key stages of M&A transactions here, and more on structuring the sale of your startup here.

Suppose you are contemplating selling your company as an investor or company founder who sits on the board. In that case, you have critical fiduciary duties to consider when making these types of big decisions.

Presumably, the highest duty known to the law, the fiduciary duty, is an obligation of loyalty and good faith to a person or entity. It requires dedication and care that does not allow a violation without exposure to personal liability. Fiduciary duties do not permit undisclosed conflicts of interest, and they also require transparent sharing of all information where even a whiff of conflict could be spotted in the rear view mirror. Before a person becomes a director of a corporation, much like the trustee of a will, it is essential to have a thorough understanding of fiduciary duties to others.

Today, a director can take the most critical steps to ensure compliance with fiduciary duties by attending every meeting, reading materials in advance, and considering the interests of all parties concerned, especially those not in the room. As a fiduciary, your actions will be viewed in hindsight with 20/20 vision.

In recent years, the intersections of personal relationships with significant business decisions have received judicial scrutiny like never before, especially related to sales of securities. In a paradigm shifting Delaware Chancery opinion, the court found that the undisclosed co-ownership of a pleasure craft among two directors (in the absence of any other factor) could potentially constitute a conflict of interest when the company upon which board the two directors served made a business decision.

When your company is for sale, your duties become heightened, and your fiduciary duties expand to include exerting best efforts to obtain the highest possible value for all stockholders. You should consider the interests of the common stockholders as “residual claimants,” therefore avoiding decision-making that benefits preferred stockholders to the detriment of the common stockholders. Often times, your hands are tied, such as when the value of the company does not exceed the aggregate liquidation preferences of the preferred stockholders. What to do?

Some companies in this situation may consider a "carve-out" of some amount of proceeds for the common stock holders (even those not comprising the current executive team required to execute the sale).

Following are simple guidelines you can follow to stay on the right side and walk the line:

- schedule regular meetings to discuss whether or not a sale transaction makes sense for the company, including analyzing the company's strategy, prospects, and value.
- do your diligence and engage skilled experts and advisors. Engaging an investment banker to run a full sales process and bring the company to market provides useful cover to demonstrate that you exerted best efforts to achieve the highest possible terminal value for all stockholders. (More about engaging an investment banker here.)
- make sure to document the process in clearly drafted minutes reflecting a thorough consideration of all factors.
- be sure conflicts of interest of directors and officers are disclosed to the board and stockholders if needed and reflected in the minutes.
- if conflicts of interest exist among board members, set up a special committee or use independent non-interested directors to provide a check and balance in the process.

The global M&A outlook in 2021 is looking very strong. Following these simple rules will go a long way to ensuring successful execution.

Louis Lehot is a partner and business lawyer with Foley & Lardner LLP, based in the firm's Silicon Valley, San Francisco and Los Angeles offices, where he is a member of the Private Equity & Venture Capital, M&A and Transactions Practices and the Technology, Health Care, and Energy Industry Teams. Louis focuses his practice on advising entrepreneurs and their management teams, investors and financial advisors at all stages of growth, from garage to global. Louis especially enjoys being able to help his clients achieve hyper-growth, go public and to successfully obtain optimal liquidity events. Louis was the founder of a Silicon Valley boutique law firm called L2 Counsel. He previously served as both the co-managing partner and co-chair of the emerging growth and venture capital practice of a global law firm in Silicon Valley.

ABOUT FOLEY & LARDNER LLP

Foley & Lardner LLP looks beyond the law to focus on the constantly evolving demands facing our clients and their industries. With over 1,100 lawyers in 25 offices across the United States, Mexico, Europe, and Asia, Foley approaches client service by first understanding our clients' priorities, objectives, and challenges. We work hard to understand our clients' issues and forge long-term relationships with them to help achieve successful outcomes and solve their legal issues through practical business advice and cutting-edge legal insight. Our clients view us as trusted business advisors because we understand that great legal service is only valuable if it is relevant, practical, and beneficial to their businesses. Learn more at Foley.com.

FOLEY

FOLEY & LARDNER LLP

FOLEY.COM

AUSTIN | BOSTON | BRUSSELS | CHICAGO | DALLAS | DENVER | DETROIT | HOUSTON | JACKSONVILLE | LOS ANGELES | MADISON | MEXICO CITY | MIAMI | MILWAUKEE
NEW YORK | ORLANDO | SACRAMENTO | SALT LAKE CITY | SAN DIEGO | SAN FRANCISCO | SILICON VALLEY | TALLAHASSEE | TAMPA | TOKYO | WASHINGTON, D.C.