41 Legal Practice Areas That Didn't Exist 15 Years Ago

Spotlight - 2018 Edition
By Carolyn Elefant
# TABLE OF CONTENTS

FOREWORD: 40 PRACTICE AREAS THAT DIDN’T EXIST 15 YEARS AGO ................................................................. 4

3D PRINTING ...................................................................................................................................................... 10

ALGORITHM LAW ........................................................................................................................................... 15

#ALTLAW REGULATION .................................................................................................................................... 17

ANIMAL LAW ................................................................................................................................................ 21

ANTI-VAX LAW ........................................................................................................................................... 23

ARTIFICIAL INTELLIGENCE, ROBOTS & SELF-DRIVING CARS ..................................................................... 27

ASSISTED REPRODUCTIVE TECHNOLOGY ................................................................................................. 31

AUGMENTED & VIRTUAL REALITY (AR/VR) ............................................................................................... 36

BIOMETRICS ................................................................................................................................................ 40

BITTORRENT LITIGATION ............................................................................................................................. 45

BLOCKCHAIN TECHNOLOGY ....................................................................................................................... 47

CAMPUS DEFENSE LAWS ............................................................................................................................. 50

CANNABIS LAW .......................................................................................................................................... 53

CLIMATE CHANGE LITIGATION .................................................................................................................. 59

COWORKING LAW .................................................................................................................................... 61

CRAFT ALCOHOL ........................................................................................................................................ 64

CROWDFUNDING ....................................................................................................................................... 67
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOCIAL ENTREPRENEURSHIP</td>
<td>153</td>
</tr>
<tr>
<td>SOCIAL MEDIA AND DISCOVERY</td>
<td>156</td>
</tr>
<tr>
<td>STUDENT LOAN LAWS</td>
<td>159</td>
</tr>
<tr>
<td>TINY HOUSE LAW</td>
<td>163</td>
</tr>
<tr>
<td>VAPING &amp; E-CIGARETTES</td>
<td>165</td>
</tr>
</tbody>
</table>
FOREWORD: 41 PRACTICE AREAS THAT DIDN’T EXIST 15 YEARS AGO
When it comes to discussion about the future of law, form dominates substance. Much of today’s thought leadership on the future of law focuses on how technology -- artificial intelligence, blockchain, the cloud, document automation and data analytics -- changes the mechanics of how we practice law. Missing from the conversation, however, is any comprehensive examination of how those same technology trends that drive legal practice innovations are also shaping and transforming the very substance of the law itself.

But why is it important for lawyers to keep abreast of the myriad of new practice areas spawned by technology either on its own, or in cahoots with its frequent companions, policy reform and social change? After all, aren’t the 41 new practice areas covered in this Guide nothing more than some version law of the horse on steroids - compendium of skinny little specialty niches that when you get down to brass tacks, are nothing more than new fact patterns readily resolved through the application of the same general legal principles that we learned back in law school?

Well, yes - and no. As I discovered after embarking on this project, technologic, policy and social forces careen so rapidly these days that they quickly bump into complex questions that stretch the boundaries of conventional legal analysis. Our slim legal toolkit for dealing with uninvented law -- basically, through application of past precedent, use of analogy and my personal favorite, reasoned elaboration (thanks, Cornell Law!) -- is hopelessly inadequate when we’re confronted with developments that turn well-understood principles on their head. Consider for example, the Fourth Amendment doctrine that any evidence in plain view during a lawful traffic stop is fair game. With biometric technology like facial or retina recognition, plain view doesn’t afford much of a privacy protection when a police officer can gain heaps of information just by snapping a photo. What about employment or disability laws that apply to most private companies - can they be bypassed when the company’s business is performed by an army of independent contractors to whom these laws don’t apply? This is a small sampling of the kinds of gaps and inconsistencies that arose in topic after topic.

LESSONS LEARNED
Below are some of my broader observations gleaned from this project and thoughts on why it’s so important for lawyers to learn more about 41 Practice Areas That Didn’t Exist 40 Years Ago.

1. **Moore’s Law** - We always speak of Moore’s Law as shorthand for the rate of change in technology. Policy reforms and social progress move at a quicker pace too. By way of example, it took almost 60 years to move from the separate by equal doctrine under Plessy v. Ferguson (1896) to the elimination of segregation in schools in Brown v. Board of Education (1954), and another 13 years to put an end to state bans on mixed race marriages in Loving v. Virginia (1967) - a total of 68 years to achieve change. Contrast that to the 30 years required to change law with respect on same sex couples - going from upholding state sodomy laws in Bowers v. Hardwick (1986) to overturning those laws in Lawrence v. Texas (2003) to legalization of gay marriage in Obergefell v. Hodges (2015). The correlation between technology progress and policy/social change is not coincidental. With technology, news of change spreads more rapidly, and up close, is no longer as threatening. Technology also results in speedier transfer of information, which can help movements like social entrepreneurship (another practice area covered to blossom simply by making the resources available to others how to do it. Rapid change is exciting - but it also forces lawyers to stay nimble to keep abreast of new trends and to responding to, or capitalize on the changes - or risk obsolescence.

2. **Lawyers Need Technical Expertise to Deal With Innovation** - Many of the 41 new practice areas catalogued - such as 3D printing, Blockchain, Internet of Things, Algorithm Law, Biometrics, Cyberbullying, Augmented & Virtual Reality, Cybersecurity, Open Source Law and Privacy, to name a few - are so complex that to they require technical expertise and support to fully understand. Thus, it’s common trend for firms dealing with these issues to have in-house expertise - either through their own background (e.g., programmer-turned-lawyer) or in-house information officers or software engineers. With collaborations between lawyers and other professional experts growing increasingly common, it may be time for the legal profession to consider relaxing rules on non-lawyer partnerships to enable law firms to more easily offer hybrid services.

3. **Innovation Looks Alike** - Although the specifics of technology, regulatory and social innovation are differ - and are critical to master, when you immerse yourself in 41 new practice areas over the course of three months as I have, obvious patterns emerge. Some deal with gaps in the law by redefining their service (e.g., Uber as a ride sharing service rather than common carrier taxi) and others by seeking reform to level the playing field (like craft beer, food trucks and tiny houses) while others (like #altlaw) still struggle with the best path forward. With some innovations, companies buy themselves time with strict arbitration clauses and strategic settlements to prevent definitive resolution of issues with damaging consequences (See Sharing Economy) while in other fields, like cyberbullying, parties may have no choice but to fight until
resolution, which at least, creates certainty. There are other patterns and tactics too, far more elegantly described in a recent paper by J.B. Ruhl, Sara Light and Eric Biber entitled *Regulating Business Innovation As Policy Disruption*, Vanderbilt Law Review. The point is that even as each niche has its own unique characteristics that must be understood at the micro-level, a common theme of innovation and disruption runs through each of the 41 new practice areas, with benefits to be gained from viewing them as different pieces of the same puzzle rather than silo'ing each practice area entirely.

4. **New Practice Areas Means New Demand for Lawyers** - With the rise of automation, solo lawyers handling a steady diet of generic matters like preparation of wills, corporate documents and uncontested divorce will soon go out of business. Lawyers can gussy up these services as much as they want, touting "exceptional client service" and error-free work, but the truth is that in ten years or less, most budget-minded folks are not going to trek down to an office and pay hundreds or thousands of dollars for a matter that they can handle online with a couple of keystrokes. And even today, when there are still clients able to pay for a helping of legal advice along with their paperwork, the competition is fierce. Today, a startup can go online to sites like UpCounsel, LawKick, Avvo and others and choose from cut rate legal service providers who can set up an LLC or draft an employment handbook. But companies needing advice on setting up a lawful cannabis industry or craft beer establishment or deciding between a b-corporation or public benefit corporation won’t readily find as many lawyers capable of doing the work - which means that those lawyers who can will command higher rates. Lawyers doing more generic consumer oriented work don’t need to jump ship and trade in a family law practice for a cybersecurity niche firm. But they can incorporate practice areas like digital assets into estate planning, social media discovery into family law, etc...to stand out from the crowd and access higher paying clients.

5. **Available Knowledge on New Practice Areas Is Not As Available As You’d Think** - Truth be told, when I embarked on this project, I thought it would be a breeze. I assumed that I could easily find law review articles or detailed blog posts summarizing key legal issues related to Cryptocurrency, Fantasy Sports, Internet of Things, Sharing Economy, Social Entrepreneurship or fill in the blank. Shockingly, for many topics, there were few legal resources and those available were pretty lame. Law firm blog posts and bar journal articles covering many of these topics either failed to link to underlying case law (thus sending me on a wild goose chase) or addressed generic obvious issues (i.e., the fact that all new technology will raise patent and IP concerns) without highlighting issues unique to the practice area. Moreover, much of the material that is available isn’t conveniently indexed or easily located - a failing that I’m optimistic that my buddies, Kevin O'Keefe and Bob Ambrogi will figure out a way to solve through their new project at Lexblog.
Even worse, most of the law journal articles that I found were even more useless than the blog posts. Some pontificated about irrelevant theoretical topics, some were flat wrong on the law and all were already 6 months out of date - which isn’t surprising, given the lead time to get to print and the pace of change (During the three months that I spent on this project, new developments and changes popped up weekly). If journals can’t stay abreast of changes and provide useful and accurate information to lawyers dealing with these issues on a daily basis, then what purpose do they serve?

6. Lawyers Aren’t Exempt from These Changes - Even as forward-looking lawyers turn to other industries for inspiration, sometimes, we forget that the practice of law itself is all part of this march towards progress. For that reason, I’ve included #altlaw regulation as one of the new practice areas, but I’ve also included bonus sections on the ethics of crowdfunding, payment by cryptocurrency, co-working and gig-economy so that lawyers can take advantage of these trends.

CAVEATS & ACKNOWLEDGMENTS

A few caveats about this Guide. First, some new practice areas are missing from the list. Although the guide covers social media in litigation, the many issues related to social media in the workplace are not covered - largely because there is already ample guidance on this topic. Similarly, topics like the Communications Decency Act (though mentioned in passing as part of some practice areas), Domain Name Law, Creative Commons Licensing and Legal issues and the Cloud were on the horizon 15 years ago and have already developed extensive case law that was too much to master in the short time this Guide was written. Even so, topics like cyberbullying, LGBT, sharing economy and 3D printers still required fairly extensive coverage.

What qualifies me to write this Guide? Well, I’ve tracked innovation and changes in the practice of law ever since I launched my blog, MyShingle.com 15 years ago. And I’ve been through the innovation cycle in my own practice several times. As a young attorney, I published an article on regulation of ocean energy, created a path (where none existed) that resulted in the first license issued for a marine energy project in the United States, and then co-founded a trade association which helped to architect the regulations later adopted that currently govern offshore wind and marine renewable projects, and raised over $100 million in appropriations for the industry through lobbying initiatives. With Nicole Black, I co-authored the book, Social Media for Lawyers, back in 2010, the first publication to teach lawyers the vast benefits of social media and show them how to ethically incorporate it into their practices. These days, you can find me pioneering constitutional challenges to shield
landowners from forced condemnation of their property by gas companies seeking to build massive pipelines that will export gas overseas while encumbering landowner property with infrastructure that will be rendered obsolete within a decade by distributed generation and renewables.

I’m a fairly quick study and swift writer, but I couldn’t produce this Guide on my own. I was assisted by two contract attorneys, Carmee Murphy, primary author of Assisted Reproduction, Campus Defense Law, Cryptocurrency, Cyberbullying, Coworking law, Genetic Testing, Lawyer Scams, Anti-Vax, LGBT, First Amendment & Online Defamation, Fantasy Sports, Open Source Law, Personal Jurisdiction, Social Media in Evidence and Student loan law and David Baake, primary author of Animal Law, Climate Change Litigation, e-accessibility, Organic Certification, Food Truck Law, Rooftop Solar and Tiny House Law.

My best role model on the importance of constant innovation was my late husband, Bruce Israel. A brilliant computer scientist, my husband studied artificial intelligence when it was still a sci-fi phenomenon back in the early 1980s, then took up new languages - C++, Java, Python, Hadoop as he worked for defense contractors, the financial industry, tech companies like Google and Amazon and a bunch of startups. Right before Bruce fell ill back in 2014, he had just completed an online certification in cryptography, at least a year before bitcoin and blockchain hit the mainstream. At a time when many programmers become less valuable with age, Bruce stayed cutting edge and in hot demand not only because of his talent but because of his insatiable curiosity enthusiasm for change which he passed on to me. When I think of innovators, I think of him.
WHAT IS IT?

3D printing, also known as additive manufacturing, is a process of making three dimensional solid objects from a digital file. 3D printing has been used in a variety of industries - from energy, airline, fashion and housing industry to print parts components to manufacturing of drugs and anatomy parts designed to match specific patients. See generally 3D Printing, Wikipedia and Thierer & Marcus, About3DPrinting; also Guns,Limbs&Toys:Futureof3DPrinting, 6 Minn J. Law and Tech. (6/2016).

WHY NOW?

The 3D printer market was $2,200 million in 2012; all reports and forecasts point to a huge growth cycle. The market is expected to hit $7,240 million by 2019, with global forecasts calling for $30.19 billion by 2022. What accounts for the recent explosion of 3D printing over the past five years? In contrast to other fields - like cannabis or Augmented/Virtual Reality, 3D printing has benefited not just from technology advancements but also the expiration of patents on certain processes - some which date to the turn of the century. See Expiring Patents Ushering In Next Generation of 3D Printing, TechCrunch (12/2106). For example, says Tech Crunch when the Fused Deposition Modeling (FDM) printing process patent expired in 2009, prices for FDM printers dropped from over $10,000 to less than $1,000, and a new crop of consumer-friendly 3D printer manufacturers, like MakerBot and Ultimaker, paved the way for accessible 3D printing. Regulatory changes - such as the FDA’s recent guidance (December 4, 2017) to manufacturers using 3D printing for medical devices - is also expected to also spur innovation by creating a framework for developing new products that can go to market more quickly.

KEY LEGAL ISSUES:

Copyright - Because 3D printers are capable of reproducing objects, the industry has an interest in understanding when an artistic feature incorporated into the design of a useful article eligible for copyright protection. For example, is a cup with a unique handle merely a nonu -copyrightable utilitarian work - or is does the handle have such a creative design that it makes the entire cup copyright protected? This
question long perplexed lower courts which established more than a
dozen competing tests, prompting the Supreme Court to take up the
issue in Star Athletica Brands v. Varsity, 137 S. Ct. 1002 (2017). There,
the Supreme Court established a uniform Court held that "a feature
incorporated into the design of a useful article is eligible for copyright
protection only if the feature (1) can be perceived as a two- or three-
dimensional work of art separate from the useful article and (2) would
qualify as a protectable pictorial, graphic, or sculptural work—either on
its own or fixed in some other tangible medium of expression—if it were
imagined separately from the useful article into which it is incorporated."
Applying this test to cheerleader costumes, the Court found that the
distinctive chevron stripes qualified as a protected pictorial work and
therefore, the uniforms—otherwise non-protected utilitarian items—
were subject to copyright protection by dint of the design. Preliminarily,
the Court’s test is expected to generate more infringement litigation at
3D design sites since many objects previously viewed as utilitarian are
arguably afforded more protection by Varsity Sports. (See Is Supreme
Court Decision on Uniforms Worth Cheering for, TechCrunch,
7/26/2017).

CAD Files & Copyright - Many users upload computer aided design files
(CAD) for creation of an object to sites like Shapeways or Thingverse to
enable others in the community to share the file or reproduce the object
for personal use. In February 2016, a firestorm erupted when a designer
names Loubie who had uploaded a CAD file for a dragon figurine
discovered that a third-party company, 3D Print was using the file to
reproduce and sell her figurine on eBay. See 3DPrint News, February
2016. Loubie’s complaint went viral, leading eBay to remove the objects
- but leaving the question of whether 3D Print’s use of the files was
unlawful. As a general matter, protection accorded to CAD files mirrors
the underlying copyrightability of the subject. In other words, if the CAD
file will reproduce a creative form subject to copyright protection, then
the CAD file itself is protected by copyright. Thus, as a copyright owner,
Loubie could control use of the underlying file as well as production of
derivative works therefrom. See 3DPrint News, August 2016. If the CAD
file produces a functional item, the level of copyright protection for the
file itself is unclear; the resulting functional object would not be subject
to an infringement claim.

DCMA Protection: What happens when a person uploads a
copyrighted CAD file to a 3D printing site like Shapeways or Thingiverse
(which print 3D objects on demand from CAD files) and doesn’t hold a
copyright for the file? While the person uploading the file may face
infringement charges for misappropriation of the CAD file, the hosting
platforms themselves have protection under the Digital Millennium
Copyright Act which grants immunity to intermediary sites so long as
they promptly remove materials in response to a takedown notice.

Derivative Works: When might a useful/functional article would be
considered a derivative work of a copyrighted design?” J. Huddelston
Skees, Read Plain Text (8/2017). Varsity Sports resolved the question of
distinguishing between functional v. creative works, but did not address
derivative works. For example, a Pokemon fan created a tiny planter based on a Pokemon character which she uploaded to Shapeways to sell - only to receive a takedown notice from Pokemon International. As Techdirt suggests, the planter might have been protected under derivative works doctrine as it only vaguely resembled the Pokemon character, and Pokemon does not sell character-inspired planters. Nevertheless, Shapeways complied with the takedown demand.

**Patents:** A recent case from the International Court of Trade sheds some light on whether CAD files produced by patented software. In ClearCorrect LLC v. ITC, 810 F.3d 1283, a manufacturer of plastic orthodontic braces was alleged to be violating of the Tariff Act which prohibits imports of infringing articles. The manufacturer was importing CAD files from Pakistan to the U.S. and used them to 3D print the braces 00 allegedly in violation of the software patent used to create the CAD files. The Federal Circuit held that the digital CAD files were not material things or articles that are patent infringement claims.

**FDA Regulations:** In December 2017, the FDA released Technical Guidelines for Additive Manufactured Medical Devices what Commissioner Scott Gottlieb characterized as “leapfrog guidance” to bridge the gap between the state of the industry today and where it will be tomorrow. Prior to releasing the statement, the FDA had reviewed more than 100 devices currently on the market that were manufactured on 3D printers, ranging from knee replacements and implants for facial reconstruction, and also approved the first drug produced on a 3D printer that was designed to dissolve more rapidly. The FDA guidance makes it the first agency in the world provide a comprehensive technical framework to advise manufacturers creating medical products on 3D printers.

The guidance addresses to main topics: Design and Manufacturing and Device Testing Considerations. The Design and Manufacturing Considerations section provides technical considerations that should be addressed as part of fulfilling Quality System (QS) requirements for your device, as determined by the regulatory classification of your device and/or regulation to which your device is subject, if applicable. The Device Testing Consideration section describes the type of information that should be provided in premarket notification submissions (510(k)), premarket approval (PMA) applications, humanitarian device exemption (HDE) applications, De Novo requests and investigational device exemption (IDE) applications for a 3D printed device.

The guidance also offers examples of how it might work in practice. For instance, a 3D printer manufacturer would need to get clearance if the software for their printer is marketed as capable of outputting 3D printed anatomical models for diagnostic use. Similarly, if a software company is marketing software as capable of creating files for making such models, the software would need to be cleared. On the other hand, clearance would not be required for printers or software marketing for creation of anatomical models for diagnostic use. Likewise, no
clearances are required for 3D printer use in medical school or clinics to create models for diagnostic or teaching purposes.

3D Printing & Guns: Generally, 3D printed guns for personal use are lawful - though subject to several caveats. 1968 Gun Control Act, people who make or sell firearms in the U.S. must be licensed and deal in firearms with serial numbers - except if the firearms are made for personal use. But California recently passed a law to require those who 3D print guns to register them. See California Passes Law Requiring Registration of Homemade Guns, Motherboard (May 2016). The Undetectable Firearms Act prohibits makes it illegal to manufacture or import guns that are undetectable through metal detectors - so to be legal, a 3D printed plastic gun must include a metal insert. Posting CAD files online for 3D printing guns that are accessible overseas is another matter. A recent Fifth Circuit case, Defense Distributed v. US Dept. of State, 838 F.3d 451 (5th Cir. 2016) involved a challenge by Defense Distributors, a 2nd Amendment nonprofit, to the State Department’s demand that the organization remove from its website CAD files for printing 3D guns until the State Department could determine whether the site violated the International Traffic in Arms Regulations (ITAR) ban on gun exports overseas. Defense Distributors argued that its rights to post the files was protected by the First Amendment. Although the Fifth Circuit did not rule on whether the CAD files were entitled to First Amendment protection, it found that even if this were true, that the State Department’s interest in protecting national security overrode constitutional considerations. The dissenting judge Edith Jones disagreed, reasoning that if it is lawful to build a gun at home, then posting files on how to do it can’t be restrained without running afoul of the First Amendment.

On July 10, 2018, the federal government reached a settlement with a 3D gun manufacturer in Texas. On July 30, 2018, seven states filed a lawsuit to prevent posting of online instructions for manufacture of 3-D printed guns. The release was blocked by a temporary restraining order for now as the Trump Administration continues to explore new regulations to allow for download of 3D gun blueprints. See Washington Post.

Products Liability: 3D printers are not yet sufficiently mainstream to have given rise to products liability claims. Some argue that existing common law principles of products liability are adequate to govern future 3D printing claims. See Thierer & Marcus, supra. Others argue that the segmented nature of the 3D production process introduces so many new parties into the chain of production that traditional products liability laws - which have traditionally applied to a single manufacturer responsible for all components - may not be capable of handling.

As discussed in 3D Printing Leaps, BNA (September 2016), 3D printing raises products liability questions such as (1) whether creation of customized products - such as prosthetics for a customer’s anatomy - can make manufacturing defects harder to detect since every 3-D
printed object is slightly different and (2) who is liable for defects - the creator of the design or the 3D printer that manufactured the item?

Future Opportunities & Trends: We have not located any products liability claims related to 3D printing - likely because many products are still being produced either at a one-off level or for specific purpose. The same is true for patent litigation - even if individuals are infringing on a patent through individual use, detection is nearly impossible on an individual level. As 3D printing becomes more widespread, patent and products liability claims may grown. Meanwhile, the new FDA regulation will create opportunities for advising everything from startups to major pharmaceutical companies on compliance on developing 3D products and processes that will survive FDA scrutiny.
WHAT IS IT?

Simply put, **algorithms** are instructions used by a computer for solving a problem or completing a task. The internet runs on algorithms - which are used for everything from online searching, online dating and book recommendations, attorney ratings and GPS mapping. See Pew Report - The Algorithm Age (February 2017).

Legal tech companies are developing algorithm-based tools to assist lawyers in predicting the strength of a potential client’s case, and indeed, may someday be used in helping lawyers to decide whether to retain a client at all.

WHY NOW?

According to the Pew Report - Algorithm Age, technology and policy experts concur that “[Use of algorithms] will continue to proliferate – mostly invisibly – and expects that there will be an exponential rise in their influence.” Because algorithmic decisions may embody bias and have serious consequences for consumers, use of algorithms has also attracted interest of policymakers. See White House Report on the rise of algorithms and AI (2016) and Congressional subcommittee hearings on risks that widespread reliance on algorithms may pose to consumers (November 2017).

KEY LEGAL ISSUES:

**Due Process Concerns** - Use of algorithms in criminal cases raises due process concerns when defendants are denied access to the methodology applied, or when the algorithms are biased. See Wisconsin v. Loomis, 881 N.W.2d 749 (2016) (rejecting defendant’s claims that lack of access to COMPAS algorithmic risk assessment tool for potential recidivism violated due process, finding that sentence was based on numerous factors in addition to the COMPAS results and that the defendant failed to show that COMPAS was gender biased), Wired Magazine (11/29/2017)(describing due process challenge to conviction based on identification of DNA through “probabilistic genotyping” formula to which defendant was denied access), But see but see Judge Releases DNA Software Source, ABA Journal (11/29/2017).

**Discrimination Concerns** - For the past four years, Chicago has relied on an algorithm to evaluate every person arrested for for risk
of future crime— which shapes policing strategy and use of force. At the same time, a Department of Justice investigation of the Chicago Police Department found that racial discrimination remains a problem, thus raising questions about whether the algorithm may reflect those biases. See Police Use Algorithms to Tell if You’re A Threat, Time, 10/3/2017. The EEOC is also investigating complaints that job tests, which rely on certain algorithms may discriminate against the mentally ill. See Do Job Personality Tests Discriminate, ABA Journal (9/30/2014).

Future Trends & Opportunities:
Algorithms are a sleeper issue, as well as a significant problem waiting to happen. As algorithms become more pervasive and gain influence in public policy, the courts and consumer matters, there is a growing need for “algorithmic literacy, transparency, and oversight.” says the Pew Report. At the same time, as algorithms become more sophisticated, courts and prosecutors will turn to them as a way to save resources— which in turn will put court-appointed and other resource-constrained criminal defense lawyers at a disadvantage— because even if they can successfully compel disclosure of algorithmic models, they may lack the expertise to challenge them. Lawyers must educate themselves on algorithms to ensure that their use does not harm their clients’ interests, and must also participate in public policy discourse on the potential consequences of reliance on algorithms without evaluating the formulas or underlying data sets for possible bias.
# ALTLAW REGULATION

## WHAT IS IT?

#AltLaw is shorthand for “alternative law companies” - a definition that encompasses those companies that are not law firms but that provide some type of law-related services - such as online document preparation, lawyer Q&A sessions or operating a platform that facilitates connection between lawyers and clients. Examples include LegalZoom and RocketLawyer (online document services), chatbot and AI sites (DoNotPay.com - offering 1000 free bots for various legal matters), UpCounsel and Priori Legal (matching small businesses with lawyers) and Avvo (Q&A service and flat fee legal services for clients) and freelance and on demand services (Axiom or Hire an Esquire - see also Sharing Economy Section). There are some who consider virtual law firms, or firms providing unbundled services within the rubric of #Altlaw. We do not consider those models in this discussion because location independent lawyers (if not virtual, then available by phone) and unbundled services have been around for decades and do not, in our view, raise novel legal issues not already addressed by existing rules. See Ethics of Virtual Law Practice, Direct Law (extensive analysis of virtual law office ethics issues).

## WHY NOW?

Stodgy lawmakers and provincial bar regulators have always clashed with new approaches to make law more affordable and accessible (recall, the Texas’ efforts in the late ‘90s to ban Nolo self-help books as unauthorized practice of law (UPL). But there differences today. First, legaltech is big business these days with $1 billion invested in legal tech startups by 2015, with the online document market doubling in value between 2006 and 2015. But regulatory uncertainty over UPL and other ethics concerns deters lawyers from participating and has stymied further growth.

## KEY LEGAL ISSUES:

**AntiTrust:** When attorney disciplinary boards prohibit non-lawyer providers from offering services that compete with traditional law firms, they may be exposed to anti-trust claims in the wake of a recent Supreme Court case, North Carolina Board of Dental
Examiners v. FTC 135 S. Ct. 1101 (2015). There, the Court found because the Dental Board is primarily composed of the same professionals active in the market it regulates and was not subject to oversight by the state, it did not qualify for antitrust immunity. Already, one #altlaw company, TICKD - an app where drivers can upload traffic tickets, pay a fixed price and receive a lawyer to defend the ticket - has initiated an antitrust suit against the Florida Bar. TICKD argues that the Bar's prolonged investigation of whether TICKD's service constitutes unlawful practice of law has emboldened TICKD's competitor, a law firm known as the Ticket Clinic - to file ethics complaints against every lawyer who has taken cases from TICKD in an effort to maintain its market share. See TICKD v. Florida Bar, 1:17-cv-24103 (11/08/2017).

On December 19, 2017, a second anti-trust suit was filed - this time by a law firm against an #altlaw providers and the state bar associations. See LegalForce RAPC Worldwide, P.C. et al v. LegalZoom.Com, Inc. et al, N.D. Cal., No. 5:17-cv-07194, complaint filed 12/19/17) LegalForce RAPC Worldwide v. Legal Zoom and various state bar associations in the Northern District Court of California Docket No. 5:17-cv-0794 (12/19/2017). Legal Force argues that the “Defendants’ unlawful and unreasonable exclusion of licensed lawyers from performing services the way LegalZoom does in the Relevant Market has injured competition in the Relevant Market and caused Plaintiffs to lose more than twenty million dollars ($20,000,000) of sales.” The suit documents the disadvantages that law firms face - including onerous advertising and trust account requirements - and seeks to allow attorneys to compete on equal footing with non-law firms, through reduced advertising regulation, hiring non-lawyers to advise on customizing trademark applications and raising outside capital.

Unauthorized Practice of Law: #AltLaw companies engaged in document prep (e.g., Legal Zoom and Rocket Lawyer) or that appear to render advice in response to a series of user responses (e.g., chatbots like DoNotPay) raise thorny questions of whether these services constitute unauthorized practice of law. (UPL). Broadly speaking, the practice of law is deemed to encompass giving advice, drafting documents that affect legal rights and representation of parties before courts, with certain exceptions that may vary state to state (e.g., in some states, a relative can advise another on a legal issue, other states allow non-lawyers to complete legal forms so long as they act only as "scriveners" and complete the form without giving advice). Although Legal Zoom forms are completed by individuals, some argue that it constitutes UPL because instead of simply providing blank forms with instructions, LegalZoom makes determinations about which form best suits the needs of the consumer based on the consumer's answers to a questionnaire, and drafts documents which include information deemed necessary by its algorithm. Several states have either declared LZ to violate UPL statutes (e.g., Janson v. LegalZoom.com, Inc., 802 F. Supp. 2d 1053, 1065 (W.D. Mo. 2011) (refusing to dismiss UPL claims, holding “A
computer sitting at a desk in California cannot prepare a legal document without a human programming it to fill in the document using legal principles derived from Missouri law that are selected for the customer based on the information provided by the customer.

North Carolina, but settlement since reached), Missouri (court declined to dismiss lawsuit alleging UPL), Washington State (settlement on UPL claims reached) and Arkansas (litigation ongoing). See C. Blades, Crying Over Spilt Milk: Why the Legal Community is Ethically Obligated to Ensure Legalzoom’s Survival in the Legal Services Marketplace, 38 Hamline L. Rev. 31 (2015).

The UPL problem is even more complicated and less settled when it comes to chatbots or AI-powered robot lawyers that apply algorithms to respond to questions or complete forms based on information provided by the consumer. See J. Pettit Legal Chatbots: Something for Nothing (August 3, 2017). The Janson court’s approach, supra suggests that chatbots or any platform for that matter - based on a computer program developed by an individual using state law principles - would run afoul of UPL. To date, many chatbots like DoNotPay involve legal matters where typically the matters are too small for a lawyer to economically handle anyway (e.g., fighting parking ticket, disputing a charge) - so there seems to be little downside to allowing bots for these matters.

FeeSharing & Paid Referrals: Although Avvo is best known as a marketing platform for attorneys, Avvo also offers legal services directly to consumers through Avvo Answers, where users pay $39 and are connected with an attorney for a 15 minute Q&A session, and Avvo Legal Services, where a potential client pays a predetermined flat fee to Avvo for legal services (e.g., DUI, estates, employment, family law and others) and is directed to a local lawyer to handle the matter. For both Avvo Answers and Avvo Legal Services, Avvo retains a percentage of the fees to cover Avvo’s administrative and marketing costs. Services like Upcounsel and Priori Legal have a similar model, but are directed at small business rather than consumers. (Interestingly, sites like UpCounsel and Priori Legal have also evaded direct bar scrutiny though they too retain a cut of legal fees paid by clients). To date, six states - NY, NJ, Pennsylvania, Ohio and North Carolina - have barred lawyers from participating in these programs (See Avvo Loses in NY But May Win in NC, BNA (8/222017). Arguments by some or all of the bars is that Avvo’s retention of a percentage of fees is unlawful fee-splitting, Avvo is not a qualified referral service and operates as a “paid referral” service. But see Bernabe, Avvo Joins the Legal Market, 104 Georgeown L.J. 184 (2017) (opines that Avvo unlikely to be deemed a paid referral because lawyers are matched to clients by computer, not individual recommending service) and Elefant, MyShingle (October 2016)(arguing that practice of retaining a fee is no different than credit card company assessing a service charge on a bill paid
by a client). To date, however, no individual bar actions have been brought against attorneys for offering services through these platforms.

Future Trends and Opportunities:

As technology costs continue to decline, legal tech startups will continue to launch with or without VC backing. In other words, legal tech is not going away even though ethics rules are uncertain and may deter investment. Moreover, the need for solutions to the Access to Justice crisis will require lawyers who can craft arguments that will advance online document prep, chatbots and any other tools that will serve individuals whose legal needs are unmet. On this front, there will also be a need for lawyers who can engage in advocacy or policy-making to change restrictive regulations where needed. In short, #Altlaw companies will be in need of legal guidance, risk management strategies and policy advice and as such, the need for creative lawyers who can navigate the regulatory minefield so as to create opportunities for these new companies will be in very high demand.
ANIMAL LAW

WHAT IS IT?

According to the Animal Legal Defense Fund, animal law is "a combination of statutory and case law in which the nature—legal, social or biological—of nonhuman animals is an important factor.” The animals in question may be wildlife, companion animals, or animals used in entertainment, research, or agriculture.

WHY NOW?

In one sense, animal law is among the most ancient of all legal disciplines. Judges have been hearing disputes about animal dowries and torts caused by animals for as long as there has been a legal system. In the United States, the first law prohibiting animal cruelty was passed in the Massachusetts Bay Colony in 1641.

Although animal law is ancient, it is rapidly changing. Part of that change is due to evolving ideas about the moral status of animals. The modern animal rights movement began to take shape in the 1970s and 1980s, with the publication of Peter Singer’s Animal Liberation in 1975 and the founding of People for the Ethical Treatment of Animals in 1980. Organizations like PETA, the Non-Human Rights Project, and the Animal Legal Defense Fund have brought legal challenges designed to advance their conception of animal rights.

The rapid evolution of animal law is also due in part to changes in the way humans interact with animals. For example, as a greater number of people with physical and emotional disabilities rely on animals for support, disputes related to service and emotional support animals have become increasingly common.

The growing prominence of animal law is seen in the increasing number of law schools that are offering courses on the subject. In 2000, only nine law schools offered such a course; in 2015, 151 schools did. Today, there are also animal law clinics at several law schools.

KEY LEGAL ISSUES:

Ag-Gag Legislation: Ag-gag laws refer to state statutes that make it illegal for someone to record and disseminate footage of what goes on in animal agriculture. Several states have enacted ag-gag laws, although in Idaho and Utah, ag-gag laws have been successfully challenged on First Amendment grounds and found unconstitutional. See Ag-Gag Laws, Wikipedia.

Animal Cruelty Laws and Commerce Clause Issues: Efforts by state and local governments to ban puppy mills can raise commerce
clause issues if the bans are applied only to out of state dogs. There may also be issues about whether local governments have the power to ban puppy mills or if their regulations is preempted by state law. In 2017, California became the first state to ban puppy mills outright. A Massachusetts law enacted in 2016 that requires anyone selling produce to provide sufficient cage space for animals to lay down, stand up and extend their limbs has been the subject of a lawsuit by 13 states. They argue that the statute is "economic protectionism and extraterritorial regulation that violates the Commerce Clause" of the U.S. Constitution, saying residents of different states will be made to "submit to Massachusetts' laws." See Mass Live, 12/13/2017.

States have also taken steps to address specific cruel practices. California banned foie gras which is often produced by force feeding birds to enlarge the size of their liver. See Wikipedia.

Changing laws on damages: While owners can recover damage for intentional killing of a pet (such as a police officer shooting a dog during a raid), typically, monetary awards for the negligent death of a pet have been low because animals are still considered to be property in most states. A lawsuit now underway in Washington D.C. seeks to change that view; as the Washington Post reports that a woman alleging that a pet boarding facilities negligence resulted in her dog’s death while in the facility’s care is seeking $150,000, arguing that her dog was not just a pet, but a companion and family member.

Custody Disputes and Pets: Traditionally, pets have been considered property when it comes to divorce cases. However, states like Alaska and Illinois have passed laws requiring judges to take into account the pet’s best interest. Pet custody disputes are a growing concern, with a report by the American Association of Matrimonial Lawyers reporting a 27% increase in such disputes in divorce cases. See AAML Press Release (2014). In 2016, Connecticut became the first state to pass legislation allowing courts to appoint legal advocates for abused animals.

Future Trends & Opportunities:
As cultural norms towards animals change, animal law will continue to grow and create new opportunities for lawyers to engage in both advocacy at both the legislative and judicial level. Opportunities include serving as a consultant to traditional law firms (e.g., PI, family law or estate planning) on animal law issues, or working with associations or nonprofits on cases that push the law on animal rights.
WHAT IS IT?

Vaccination law deals with a range of issues, from challenges to school decisions to bar non-vaccinated children from admission to claims before the specialized Vaccine Court for compensation for harm caused by vaccines.

WHY NOW?

Although vaccine controversies - or the anti-vaccine movement date back to the 1700s, they’ve gained new attention as a result of well-publicized claims of a link between vaccination and autism that emerged in the early 2000’s - and have since been rejected by the Vaccine Court in three “test” cases. See Cedillo v. HHS, No. 98-916V (Fed. Cl. Spec. Mstr. Feb. 12, 2009), aff’d, 89 Fed. Cl. 158 (2009); Hazlehurst v. HHS, No. 03-654V (Fed. Cl. Spec. Mstr. Feb. 12, 2009), aff’d, 88 Fed. Cl. 473 (2009); and Snyder v. HHS, No. 01-162V (Fed. Cl. Spec. Mstr. Feb. 12, 2009), aff’d, 88 Fed. Cl. 706 (2009). Cedillo and Hazlehurst were affirmed again on appeal by the U.S. Court of Appeals for the Federal Circuit (see Hazlehurst, 604 F.3d 1343 (Fed. Cir. 2010); and Cedillo, 617 F.3d 1328 (Fed. Cir. 2010)).

Still, with celebrity support and pervasive, the anti-vaccination movement persists, prompting many states to tighten their laws regarding permissible vaccine exemptions. In 2015, California passed legislation requiring virtually all California schoolchildren to be vaccinated against a range of diseases in order to attend school regardless of the personal or religious beliefs of their guardians; following, there was a drop of more than 3,000 exemptions. But in a number of other states, nonmedical exemptions have continued to rise. In 11 states (CT, FL, IW, KY, MD, NY, NC, ND, OH, OK, and VA), the number of kids not being vaccinated for nonmedical reasons is higher than at any point in the past five years.

KEY LEGAL ISSUES:

Constitutionality: Recently, three parents challenged the requirement when their children were prohibited from going to school due to the rule children must be vaccinated from going to school unless they receive a proven religious exemption, but in the event of an outbreak, those children not vaccinated may be excluded from school; at the time, two of children receive a religious exemption and all three were prevented from attending school during a chicken pox outbreak. The Second Circuit first upheld the New York requirement that school children must be vaccinated as
constitutional, rejecting the claim of violation of substantive due process, based upon the Supreme Court’s Jacobson decision (vaccination is a proper exercise of the State’s police power); and rejected arguments that an alleged growing body of scientific evidence against vaccinations altered this rule. See Phillips v. City of New York, No. 14-2156 (2d Cir. 2015). Next, the Second Circuit upheld the state’s rule to exclude non-vaccinated children from school during an outbreak as constitutional, rejecting the claim that it burdened the free exercise of religion. The Second Circuit held that the rule was neutral and of general applicability, and the State need not show a compelling government interest even if there was an incidental burden on religion, and relied upon the Supreme Court’s statement (in dicta) in Prince v. Massachusetts, 321 U.S. 158 (1944), that “[t]he right to practice religion freely does not include liberty to expose the community or the child to communicable disease or the latter to ill health or death.” Most importantly, the Supreme Court declined to hear an appeal of the case, thereby allowing the ruling to stand. See id., cert. denied, 136 S. Ct. 104 (2015).

**Family Law Issues:** - there are two divorce cases pending in Oakland County, Michigan, Circuit Court (both before Hon. Judge Karen McDonald), regarding divorced parents’ right to vaccinate their child, which are receiving media attention. Bredow adv. Horne (jailing mother for failure to vaccinate her son as contempt of prior ruling)(October 2017), Matheson adv. Schmitt (addressing dispute between parents regarding vaccination of children).

**Legal Exemptions:** Some vaccine litigation revolves around whether the party objecting falls within the state law exemptions. State laws establish vaccine requirements and enforcement mechanisms for school children (public, private and daycare facilities), but do permit exemptions such as medical, religious, philosophical, and, at times, proof of immunity. Recently, there have been lawsuits against schools that refused to admit unvaccinated children.

**Medical:** All 50 states allow medical exemption to vaccination, written by medical doctor (M.D.) or doctor of osteopathy (D.O.) (note: some states permit other state-designated health care workers to certify, but most states do not allow a doctor of chiropractic to certify); some states may require an independent review of the offered certification by an appointed doctor or health-care professional. It can be difficult to obtain a medical exemption, and is usually based upon determination of auto-immune disorder or other physical inability to receive the CDC recommended vaccine.

**Religious:** A person claiming a religious exemption must be prepared to defend the request and explain the underlying religious or spiritual beliefs; it is intended for people who hold a sincere religious belief opposing vaccination to the extent that if the state forced vaccination, it would be an infringement on their constitutional right to exercise their religious beliefs. Some states may require a letter from the head of your religious institution affirming the sincerity of beliefs and that vaccination is against the practice of the institution.
**Philosophical/Personal:** This type of exemption is for individuals who hold conscientious objections to one or more vaccines (note: less than half of the states permit this). These laws create a very low bar for parents to obtain an exemption; some simply have to check a box declining vaccination; some states require parents or children old enough to give consent (usually age 12 or older) to object to all vaccines and not just one vaccine; in Washington and Oregon, parents seeking a personal belief exemption must first obtain a signature from a medical doctor or other state-designated health care worker in order to file the exemption or may be required to complete a state vaccine education program (Oregon).

**Immunity:** Some state laws allow individuals to be exempted from vaccination or re-vaccination, if proof of existing immunity for certain diseases can be shown by a blood tier test to show there are enough antibodies present to be immune to a particular disease; private medical labs perform the test and report the level of antibodies, which report is submitted with your exemption request.

**Vaccine Court:** Any claim against vaccine manufacturers can only be heard in the vaccine court, by a Special Master without a jury. Since its first case in 1988, the vaccine court has adjudicated more than 16,000 petitions (dismissing approximately two-thirds of the cases), and has awarded approximately $3.6 billion to successful petitioners and their counsel; currently the court’s VICP is valued at approximately $3.7 billion. According to the court’s data, bona fide vaccine injuries are rare, and from 2006 to 2016, for every million vaccine doses eligible for compensation, only one injury victim was actually compensated. The vaccine court has its own procedural rules; and the statute of limitations is the three (3) years from the date of first onset of symptoms and two (2) years from the date of death for all parties (i.e., no tolling provisions); evidence of the date of first onset of symptoms is necessary to be eligible. All legal fees for cases filed “in good faith with a reasonable basis” are paid separately by the vaccine court and distributed upon petition from the VICP.
Future Trends & Opportunities:

Vaccination law is still a highly specialized practice area both due to the nature of the law and the unique system for adjudicating claims. Future litigation is possible if additional science suggests a link between vaccinations and other disease but otherwise the case work will remain stable. However, given the rise in challenges to school admissions policies (which are resolved through the ordinary court system, not the vaccination court), anti-vax law could be an interested add-on for attorneys handling special education law or other issues related to schools and accommodations.
ARTIFICIAL INTELLIGENCE, ROBOTS & SELF-DRIVING CARS

WHAT IS IT?

Artificial intelligence, robots and self-driving cars are all sub-sets of an umbrella catch-all, automation. Automation - defined as the technology by which a process or procedure is performed without human assistance - has been around for years in the form of timer-enabled appliances, cruise control, Roombas and auto-responders for email campaigns. What’s changed over the past 15 years, however is that technology advancements in the field of artificial intelligence have birthed a new generation of sophisticated automated machines such as self-driving cars, surgical robots and chatbots - capable of learning and refining performance based on prior input. As machines that impact our daily lives become intelligent, they test the limits of our existing laws and require an evaluation of whether new regulatory systems are necessary.

WHY NOW?

The rise of AI is fueled by two factors. First, and most obviously, technology advances drive Al but so too does big data which enables machines to learn faster and more effectively. At the same time, big data also creates demand for intelligent systems that can glean meaning from raw data. See generally J. Canton From Big Data to Artificial Intelligence, Huffington Post (7/5/2016). also the which in turn, have and drawn investor interest. A recent Artificial Intelligence: The Next Digital Frontier, McKinsey (June 2017) estimates that companies spent between $26 billion to $39 billion on AI systems in 2016, with highest adoption rates in high tech, telecom and financial services. The mobile robotics market is likewise poised for growth, with global spending on robotics (ranging from software and hardware to robotic receptionists and service providers) expected to reach $135 billion by 2019, according to Fortune (2/24/2016). Self-driving cars, whose performance is improved by AI (P. Els, How AI Is Making Self-Driving Cars Smarter, Robotics Trends (2016)) is also a growth market, with F10 million self-driving cars expected to take to the roads by 2020. See Forbes (3/3/2017). Finally, chatbots are another type of AI development gaining popularity. Chatbots are still in their nascency but use is expected to surge in the coming years. A 2017 survey reports that 80% of businesses want a chatbot in place by 2020.

KEY LEGAL ISSUES:
Tort & Products Liability: To date, most cases involving tort liability and robots are capable of resolution under traditional liability principles - with plaintiffs arguing negligent design or failure to warn and the manufacturer attempting to attribute blame to human factors - e.g., use of a product in a manner not intended. A recent lawsuit against Da Vinci, a robot operated by doctors through use of a joystick and employed in surgery is instructive. Trial Begins Over Allegedly Defective Robot, CVN.com (April 2016). The plaintiff - who was injured during hysterectomy surgery - argued that the company failed to warn her of FDA findings regarding DaVinci’s dangers, or to take notice of the harm caused by the device in other cases across the country. The Da Vinci manufacturers argued that the damage was caused by the plaintiff’s failure to follow her doctor’s instructions post-surgery. The case ultimately settled.

The results of NTSB’s investigation into a fatality involving a self-driving Tesla suggest that until automated systems improve, both man and machine may share responsibility for injury. In the Tesla case, the car’s driving manual states that the self-driving system should only be used on highways with clear lane markings and medians. The driver, however, did not heed this warning and when a tractor trailer crossed into the Tesla’s lane, the system did not recognize it, causing a crash that instantly killed the driver. Nevertheless, NTSB concluded that the driver was not entirely at fault because Tesla’s design lacked sufficient controls to compensate for user abuse. See NTSB Investigation of Tesla Autopilot Crash, Wired, 9/13/2017.

As robots and self-driving cars become more sophisticated, traditional tort principles may not be sufficient for resolution of claims. Consider, for example, a legal chat bot operating in accordance with rules developed by attorneys but that gives an inaccurate response to a user. Under tort law, the bot would not be liable for legal malpractice - but should it be? Consider further that the bot boasts of attorney involvement in development - does that representation heighten the standard of care? Once robots become sufficiently advanced that they can operate largely free of human interference, the issues raised with respect to liability may require a new paradigm for resolution. See e.g., R. Calo, Robotics and Lessons of Cyberlaw, 103 Cal. Law Rev. (2015) (arguing that existing tort law not capable of resolving future issues relating to robots); B. Browne, Self-Driving Cars: On the Road to a New Regulatory Era, Journal of Law Technology and the Internet (2017)(suggesting need for new regulatory regime to govern self-driving cars).

Robots & Copyright Law: Currently, robots are not eligible to hold copyrights. The latest edition of the Copyright Office’s Compendium states that “[the office] will not register works produced by a machine or mere mechanical process that operates randomly automatically without any creative input or intervention from a
human author.” Without copyright protection, works created by AI machines, for which the human author of the machine is not directly responsible, fall into the public domain. But Kalin Hristov argues that the Copyright Act is outdated and may limit the willingness of programmers and owners of AI devices to invest resources in the future development of AI if they cannot potentially gain copyright protection. See Hristov, Artificial Intelligence and the Copyright Dilemma, 57 IDEA 431 (2017).

**Autonomous Vehicles and New Laws:** For some innovation, new laws are needed to fill gaps and resolve uncertainty. For example, Wisconsin, Idaho and Virginia have all enacted laws allowing delivery bots to operate statewide. See Wisconsin Legalizes Delivery Bots, OnMilwaukee.com (June 23, 2017). On the other hand, in December 2017, San Francisco adopted rules that crack down on cargo and delivery bots: companies are limited to three robots a piece, with nine total for the City. Bots are also relegated to low population industrial areas, can’t travel more than three miles and hour and require human monitoring. See San Francisco Made Things Much Tougher for Robotic Delivery Startups, TechCrunch (12/07/2017).

Regulation of self-driving cars is far more complicated. Currently, DOT has issued guidelines and best practices for self-driving cars (See NHTSA Guidance (2017) - though this latest iteration has been criticized for removing best practices on privacy which earlier versions included. the General Accounting Office (GAO) also released a report entitled, Automated Vehicles: Comprehensive Plan Could Help DOT Address Challenges (November 27, 2017) which recommends that “The Secretary of Transportation should develop and implement a comprehensive plan to better manage departmental initiatives related to automated vehicles.” Both the GAO report and a Congressional Research Service (CRS) Report on Issues in Autonomous Vehicle Deployment, (September 19, 2017) reference existing regulatory tools and model state policies to address challenges of self-driving vehicles.

**Criminal Conduct:** Last year in Switzerland, a chatbot was arrested, reported VentureBeat. The bot’s coders deployed it to spend $100 in Bitcoin each week on the darkweb. As programmed, the bot returned counterfeit and illicit products which were displayed at a public auction, at which point the bot was arrested. The incident raises legal questions such as (1) are bot developers exempt from liability if ownership of the algorithm cannot be conclusively proven, (2) could bot developers be made liable for crimes committed by the bots if they can’t convince the authorities that the codified avatar (bot persona) was acting autonomously or in the public interest and (3) could a bot develop artificial intelligence outside the developer’s (original) control, such as while operating independently in open source environments and interacting live with humans who influenced its bad conduct or caused it to make bad decisions?
Data & Privacy: Because many AI-powered systems collect information from users (e.g., a medical diagnosis chatbot seeking information on symptoms) either to provide assistance or improve performance of the system, they raise the same privacy concerns as IoT devices. See Sections on IoT, Cybersecurity & Data Privacy.

Future Trends & Opportunities: AI-powered robots, chatbot and self-driving cars is still very much an emerging industry - and fully intelligent systems independent of any human intervention are still a few years off. For that reason, this is a great field to get involved in at the ground floor, with an opportunity to help shape the law as these technologies evolve. AI, Robots & Self-Driving cars also raise more complex questions that may require policy resolution - such as whether intelligent can operate with mens rea, practice law or medicine (and if so, will they need a license?) and similar issues.
ASSISTED REPRODUCTIVE TECHNOLOGY

WHAT IS IT?

Assisted Reproductive Technology ("ART") is used to treat fertility issues with the intention of resulting in live birth infants. Almost every part of ART is regulated by legislation to protect doctors, parents, donors, surrogates, and children. In the U.S., the federal government regulates all drugs, medical devices, and reproductive tissue used in ART; states license the practitioners (like all medical professionals) and govern insurance coverage and matters like embryo custody. ART pushes the limits of existing family or adoption law because many innovations - such as embryo custody or sperm donation - were never contemplated under existing laws and precedent.

WHY NOW?

As technology improves, ART has declined in cost and become more accessible to more people. Social trends drive growth too, including: (1) individuals marrying older and having children later in life and needing reproductive assistance, (2) reduced social stigma for parenting solo by choice and (3) rise of LGBT couples seeking to parent. According to the Centers for Disease Control and Prevention ("CDC"), as well as a report by the Society for Assisted Reproductive Technology (available: https://www.cdc.gov/art/index.html), there are more than 464 ART clinics in the U.S., and at least a million U.S. babies have been born using lab-assisted techniques; today, approximately 1.6% of all U.S. infants born every year are conceived using ART.

KEY LEGAL ISSUES:

Insurance Coverage: 15 states have some type of mandate for infertility insurance coverage - and coverage varies by state, with some having more requirements and limitations (e.g., does not include use of donor sperm or egg; age cut-offs; or coverage caps). Some states have laws that require insurance companies to cover infertility treatment, including IVF, but can limit how many cycles will be covered; other state only include coverage for certain types of treatments. Others prohibit the exclusion of coverage for a medical condition otherwise covered solely because the condition results in
infertility. In states without any mandate, most insurance plans do
not provide much coverage for fertility services, although employers
still opt to offer some infertility health insurance benefits (e.g., in
Wisconsin, there is some coverage for diagnostic testing, or Utah
requires insurers providing coverage for maternity benefits and
indemnity benefit for adoption or infertility treatments).

**Surrogacy Laws:** There are no federal regulations regarding
surrogacy; however, each state has its own regulations. Some
states have statutes permitting and recognizing paid or unpaid
surrogacy contracts; grant pre-birth orders regardless of marital
status, sexual orientation or, in some instances, genetic relationship
to the baby. Others permit surrogacy (either through statute or
having no prohibitions thereto), but have different levels of
protection for surrogates or intended parents depending on the
county, marital status or genetic relationship to the baby. Some
states do not recognize or enforce surrogacy contracts and have
statutes or decisional law prohibiting compensated surrogacy.
Lastly, there are states where surrogacy may be practiced, but there
are additional legal obstacles (including not enforcing surrogacy
contracts) or unclear laws, and pre-birth orders may not be granted.

**Donor Laws:** Most sperm donors remain anonymous, though while
many states allow sperm banks to release the donor’s identity once
the child reaches age 18 or 21, there are no laws forbidding
anonymous donation - though donor offspring have claimed a right
to know their biological donor. Almost every state laws preventing
anonymous donors from asserting legal rights such as visitation or
parental rights but strict compliance with laws governing sperm and
eyeg donation are required to determine the donor’s legal rights
unless a co-parenting or donor agreement is entered into by the
(male who donated sperm to female for an at-home insemination
was found to be the father where statute required donated sperm to
be provided to a physician); compare Steven S. v. Deborah D., 127
Cal.App.4th 319 (2005) (unmarried male who provided his sperm to
physician to inseminate his girlfriend in Massachusetts was not the
father of the resulting California child where the Massachusetts
statute required recipients to be married). Rarely, a donor will be
held to owe parental obligations, such as child support. See, e.g.,
Ferguson v. McKiernan, 596 Pa. 78, 940 A.2d 1236 (Pa. 2007)
(reversing lower court ruling requiring sperm donor to pay child
support because of an oral agreement not to hold donor liable for
support payments). Other states have legislatively stated the
donor’s responsibilities, but only in terms of husbands and wives
(e.g., Virginia law states that a donor is not the parent of a child
conceived through ART unless he is the mother’s husband) or
Maryland (child conceived through ART of a married woman with
the consent of her husband is deemed the legitimate child of both,
and the husband’s consent is presumed). A few states allow for
more than 2 persons to be recognized as legal parents. See, e.g.,
Jacob v. Shultz-Jacob, 923 A.2d 473 (Pa. Super. 2007) (sperm donor had legal obligations to support children, just like any other parent, when the lesbian couple was divorcing because donor contributed money to the benefit of the children in the past, visited the children and was known to the children as “Papa;” ruling based in part on legal precedence that same-sex partners who assume parental duties are liable for child support of tradition equitable estoppels theories).

Frozen Embryo Custody: States have different laws to determine custody of frozen embryos. In some states, absent a prior agreement regarding the disposition of pre-embryos, the party wishing to avoid procreation should prevail if the other party had a reasonable alternative option for becoming a parent. Many states opt for contractual enforcement, with others require mutual consent before embryos can be disposed of or used. See, e.g., In re Witten, 672 N.W.2d 768 (Iowa 2003); Davis v. Davis, 842 S.W.2d 588 (Tenn. 1992); and Kievernagel v. Kievernagel, 166 Cal. App. 4th 1024 (2008). In general, courts have not forced divorcing spouses to procreate against their wishes. See, gen., Reber v. Reiss, 42 A.3d 1131 (Pa. Super. 2012) (divorcing wife was given permission to use embryos created during the course of the marriage despite husband’s objections); compare A.Z. v. B.Z., 431 Mass. 150 (2000) (“[a]s a matter of public policy, we conclude that forced procreation is not an area amenable to judicial enforcement”); In re the Marriage of Rooks, 2016 COA 153 (2016) (court held that husband’s interest in not having more children outweighed wife’s interest in having more); Findley v. Lee, Case No. FDI-13-780539 (Sup. Ct., San Francisco Co., 2015) (court sided with divorcing husband where couple did not yet have any children); McQueen v. Gadberry, 507 S.W.3d 127 (Mo. Ct. App. 2016) (court determined that embryos were “marital property of a special character” and could not be used without consent of both parties); but see also Gladu v. Boston IVF, 32 M.L.W. 1195 (Mass. 2004) (during pendency of divorce, wife impregnated with frozen embryos without husband’s knowledge). Also, typically the opposing party in the case of unmarried couples prevails. But see Szafranski v. Dunston, 2015 IL App (1st) 122975-B (Ill. App. Ct. 2015), app. den’d, 2015 Ill. LEXIS 1206, 396 Ill. Dec. 186 (2015) (awarding sole custody of embryos to woman over objection of the father-donor, finding that embryos represented last opportunity for woman to have a biological child with her own eggs, and that embryos had been conceived for that very purpose), also Loeb adv. Vergara, (involving non-married parties creation of embryos in California and effort by father to obtain custody, including establishing trust in Louisiana for embryos and asserting on their behalf their “right to life; dismissing suit filed in Louisiana for want of personal jurisdiction).

In cases of married couples using donor material, courts have previously held that the embryo preference for one progenitor should be considered first then by any agreement between the parties. See, gen., e.g., Davis v. Davis, 842 S.W.2d 588 (Tenn.
1992); and Litowitz v. Litowitz, 146 Wn.2d 514 (Wash. 2002), also Wilson v. Delgado, (appeal is pending in the Georgia Supreme Court (S17A0797)) (granting custody of to ex-husband of embryos using his "genetic material" and donor sperm, and rejecting ex-wife’s custody claim under the state’s “Option of Adoption” statute, which explicitly allows both embryo donation and post-birth adoption of a child born from a donor embryo).

Pre-implementation genetic diagnosis (PGD) and Gender Selection: PGD is a process of screening embryos for genetic disorders (such as muscular dystrophy or Down Syndrome), and removing and discarding those with genetic abnormalities prior to the transfer process. In addition, the intended parents can choose the gender of the baby (either through sperm sorting or transfer of embryos of desired sex) to prevent sex-linked inherited genetic disorders (e.g., hemophilia can only be transferred from an affected mother to son). Only New York regulates the genetic tests used in PGD. Plaintiffs rarely succeed, however, in tort actions (such as negligence, medical malpractice, product liability, or emotional distress) arising out of fertility treatments and failed PGD practice; although, some trial courts attempt to shoe-horn traditional tort remedies into the case in an effort to provide some financial relief to burdened parents. See, e.g., gen., D.D. v. Idant Labs., 374 Fed. Appx. 319 (3d Cir. 2010); Donovan v. Idant Labs., 625 F. Supp. 2d 256 (E.D. Pa. 2009); Andrews v. Keltz, 15 Misc. 3d 940 (Sup. Ct., New York Co., 2007); Paretta v. Med. Offices for Human Reproduction, 195 Misc. 2d 568 (Sup. Ct., New York Co., 2003), app. withdrawn, 2004 N.Y. App. Div. LEXIS 4556 (1st Dept. 2004) (“[a] child who is conceived by in-vitro fertilization does not have a protected right to be born free of genetic defects”); Johnson v. Superior Court, 101 Cal. App. 4th 869 (Cal. Ct. App. 2002).

Posthumously conceived ART children: In the U.S., some states allow the use of frozen sperm after a donor’s death. However, it raises issues of inheritance and rights to survivor benefits. At this point, only Colorado, North Carolina and Utah statutes answer this question directly (their answers are yes, as long as the child is born within 45 months of his death). See also, Eng Khabbaz v. Comm’r, Soc. Sec. Admin., 155 N.H. 798 (2007) (no posthumously IVF conceived child was a "surviving issue" within the plain meaning of the intestacy statute); Astrue v. Capato, 566 U.S. 541 (2012) (posthumously IVF conceived children had no right to survivor social security benefits); and Beeler v. Astrue, 651 F.3d 954 (8th Cir. 2011) (under Iowa’s prior intestacy law (which have since been changed), posthumously IVF conceived children had no right to insurance benefits).
Future Trends & Opportunities:

More states will likely pass laws to address the growing issues of adoption and custody issues related to Assisted Reproductive Technology. Moreover, advancement of technology will produce new issues - such as legality of cytoplasmic transfer (now banned in the US) which results in “three person” DNA or cloning, which requires FDA approval although to date, no approval has been given. In short, technology will continue to drive change in the law of ART, making it an exciting opportunity for lawyers.
WHAT IS IT?

Virtual Reality (VR) is the use of computer technology to create a simulated environment. VR places users inside an experience, where they are immersed in a three dimensional world. Perhaps the best known example of VR is Oculus Rift, a virtual reality headset developed by Oculus, a company since acquired by Facebook for $2 billion in March 2014. See https://en.wikipedia.org/wiki/Oculus_Rift. Google Cardboard is an inexpensive VR device, fashioned from cardboard that allows users to experience VR on their smartphones.

By contrast, Augmented Reality (AR) is a technology that superimposes a computer-generated image on a user’s view of the real world, thus providing a composite view. AR gained visibility with the release of Pokemon Go - a viral game that uses the player’s smartphone GPS to locate and capture real creatures which appear on the screen as if they were in the same real life location as the player.

Somewhere between VR and AR are holograms: a 3-D, free-standing image created with photographic projection that does not require a special viewing device. Holographic technology has been used to reincarnate now departed performers like Tupac Shakur or Frank Zappa on stage (See Frank Zappa Hologram to Go on Tour, CNN (9/21/2019), or to make concerts by live performers more accessible at venues like Hologram USA, where visitors can attend concerts by performers both living and dead for around $20 a ticket.

WHY NOW?

VR and AR technologies are poised to explode over the coming years. A 2017 study by the International Data Corporation forecast global revenues for AR/VR to reach $13.9 billion by 2017, an increase of 130.5% over the $6.1 billion spent in 2016 and will reach $143 billion by 2022. The VR/AR market will only continue to grow as applications move beyond the consumer sector to industries like healthcare (where VR is used for, among other things, therapy for chronic pain and advancing autism treatment), fashion and scientific research. See https://venturebeat.com/2017/11/29/htc-invests-in-26-new-ar-vr-startups-through-its-vive-x-accelerator/. Virtual pornography is expected to be one of the top three VR uses by 2025. As AR and VR technologies advance into a myriad of industries they raise new legal questions that require resolution.
KEY LEGAL ISSUES:

**IP:** Like all other technology innovations, VR/AR raise a host of generic IP questions related to patent and/or copyright infringement and trade secret theft, and the same tests for determining unlawful use are not likely to differ significantly in VR and AR cases. See e.g., *The Whole Oculus Lawsuit Hinges on What Makes Code New Code*, Wired (January 2017)(describing that test for determining differences in code for purposes of infringement claims, while complex, does has been developed for some time). Many of these issues arose in a high-profile case by Zenimax, a video game company against Facebook alleging theft of trade secrets and infringement for use Oculus technology that Zenimax claimed its former employee had developed on the job. A jury absolved Facebook of the misappropriation claims, but found that the former employee Carmack violated the terms of his NDA and that portions of the code used infringed on Zenimax’s copyright and awarded Zenimax $500 million.

**Tort Liability:** Because AR and VR technologies are relatively new, they may have unexpected consequences that potentially give rise to products liability or consumer protection claims. Following release of Occulus VR and AR, many users reported feeling nauseous on various ratings sites - and there are even greater concerns that the devices could cause eye damage or irreversible cognitive harm. Any of these impacts could potentially trigger product liability claims, particularly if undisclosed. See Roy Bagheri *Virtual Reality: the Real Life Consequences*, UC Davis BLJ Vol. 17-1 (2016).

Are creators of AR/VR claims liable for inducing trespass? In August 2016, a class action for trespass, nuisance and unjust enrichment was filed in the Northern District of California by New Jersey homeowner against Pokemon’s developer. See *Marder v. Niantic*, Case 4:16-cv-4300. The owner argued that the games GPS coordinates lead strangers to his house who rang the bell for directions and took pictures outside his home, forcing him to deal with these intrusions while the company generated profits. Similar class actions have been filed in Michigan and Florida. See *Pokemon Virtual Trespass Suits*, SlashGear, (April 2017).

Finally, Volokh and Lemley raise the possibility of suits for virtual torts that occur within virtual worlds - such as defaming or sexual harassment of one avatar by another. See *Tort Liability: Law, Virtual Reality and Augmented Reality*, Mark Lemley & Eugene Volokh, 166 U PA. L. Rev. (2018)(extensive discussion of virtual tort issues)

**ADA Issues:** Keith Lee opines at *Associates Mind* that VR and AR technologies, like websites, are likely to be subject to the ADA, and will probably not be able to demonstrate “undue hardship” that might justify an exemption. To date, however, we are not aware of any ADA litigation against AR/VR companies. See also E-accessibility section.
**Trademark and Rights of Publicity:** Use of holographic celebrity images on stage or in VR worlds or video games raise issues such as trademark dilution and the right of publicity. See S. Anson *Hologram Images and the Entertainment Industry: New Legal Territory*? 10 Wash J. of Law and Technology, Issue 2 (2014). The First Amendment protects a clear parody of a celebrity or a “transformative” image, i.e., one that is significantly different from the underlying person (See Volokh & Leming, Virtual & Augmented Reality at 56-58, supra), but does not extend to non-transformative expansion of public figures’ rights of publicity (as argued by Anson, supra) or more robust protection for this expression under the First Amendment as Volokh and other scholars have argued in their in support of a cert petition asking SCOTUS to reverse *Davis v. Electronic Arts*, 775 F.3d 1172 (9th Cir. 2015) (holding that publicity rights trump First Amendment)? Stay tuned as this issue plays out.

**Regulation on Government Property:** Can a government entity limit access to AR game players who run amok, causing congestion and noise, and leaving trash in their wake? Perhaps - but any regulation must comply with the First Amendment, ruled a federal court judge in *Candy Labs v. City of Milwaukee*, 17-cv-569 (E.D. Wisc. 2017). There, the court temporarily enjoined enforcement of a Milwaukee ordinance that required AR gamers seeking to use the park to apply for a permits and secure garbage collection, security, and medical services, as well as insurance or face a fine or jail time. The court found that AR games qualified for First Amendment protection like ordinary video games (per *Brown v. Entm't Merchs. Ass'n*, 564 U.S. 786, 790 (2011)), and concluded that the ordinance was overbroad and incongruent with the problem it purported to solve by treating occasional and spontaneous gaming developers “as though they are trying to hold an event” in the park. The City has since settled to the case, agreeing to a permanent injunction.

**Privacy:** Mobile VR and AR devices raise the concerns regarding locational privacy and tracking. For other privacy issues related to collection of user information, see sections on IoT, Cybersecurity & Data Privacy and Biometrics.
Future Trends & Opportunities: VR and AR are emerging technologies, moving at lightning speed. The law on issues like trespass and tort, First Amendment protections will continue to evolve, making this practice area a good future opportunity.
**BIOMETRICS**

**WHAT IS IT?**

The term “biometric” derives from Greek words, bio (meaning life) and metric (to measure. See Biometrics Definition, TechTarget.com. Biometric identification refers to any technology that relies on intrinsic physical or behavioral traits to either identify you or authenticate your identity. When used for identification, an image is run against a database of images. For authentication -- such as to access a protected account - an image has to be accessed from the device to confirm a match. See generally A. Glaser, Biometrics Are Coming Along With Serious Security Concerns, Wired (3/2016).

There are two primary types of biometric identifiers: physiological, which relate to the composition of the user, such as fingerprints, facial recognition, iris recognition, retina scanning, voice recognition and DNA matching. Behavioral identifiers encompass the unique ways that individuals act such as gait or gestures. See Biometrics Definition, supra.

**WHY NOW?**

Law enforcement has been using fingerprints to identify and track people for over a century. So why are biometrics such a hot topic now? Several reasons. Not surprisingly, technology advances have improved biometrics identification systems and reduced the cost, making them more widely accessible. The technology is advancing rapidly too: whereas back in 2013, when Apple’s iPhone 5s became one of the first phones to feature a fingerprint scanner, today, virtually every consumer electronic device - smartphones, tablets and smart home controls can be accessed through fingerprint or voice recognition. Businesses are incorporating biometrics too, using the data to track worker time and attendance.

Increased concern over security is another factor contributing to the growth of the biometrics sector. Many view biometric identification (such as fingerprint scans) as a solution to lengthy airport security lines. A recent survey by Visa revealed that 46 percent of consumers polled view biometrics as more secure than passwords or PINS for verifying identity, and 50 percent view biometrics as more convenient than storing multiple passwords.

On the flip side, biometric identification raises significant privacy concerns. Alvaro Bedoya, quoted in a Wired article best
characterized why biometrics - though not inherently invasive - feel that way. Bedoya explained that "A password is inherently private. The whole point of a password is that you don’t tell anyone about it. Biometrics, on the other hand, are inherently public..."I do know what your ear looks like, if I meet you, and I can take a high resolution photo of it from afar. I know what your fingerprint looks like if we have a drink and you leave your fingerprints on the pint glass." Moreover, when facial recognition is used in law enforcement context - such as use of facial recognition to bar shoplifters from a store - the resulting harm of misidentification can be significant.

In 2015, the General Accounting Office published Facial Recognition Technology: Commercial Uses, Privacy Issues and Applicable Federal Law. GAO-15-621 in response to the proliferation of information resellers--companies that collect and resell information on individuals--which dramatically increased the collection and sharing of personal data for marketing purposes, raising privacy concerns among some in Congress. The GAO recommended that Congress should consider strengthening the consumer privacy framework to reflect the effects of changes in technology and the increased market for consumer information. At the same time, GAO cautioned that any changes should seek to provide consumers with appropriate privacy protections without unduly inhibiting commerce and innovation.

KEY LEGAL ISSUES:

Standing: As with privacy and data breach cases (See Privacy Section), at least one reported biometrics case was dismissed on standing grounds. See Santana v. Take-Two Interactive Software, No. 17-303 (November 21, 2017). There, a user sued Take-Two, developer of a video game with a feature that allows players to scan their face into the game to create a personalized avatar. The user argued that the disclosure was inadequate under Illinois Biometrics Privacy Act. The Second Circuit affirmed the lower court’s dismissal, holding that the complaint failed to raise a material risk of harm and thus, did not satisfy standing requirements under Spokeo. See also Rosenbach v. Six Flags Entertainment Corporation, Docket No. 2-17-0317, Appellate Court of Illinois, Second District (Dec. 21, 2017)(holding that a plaintiff who alleges only a technical violation of the statute without alleging some injury or adverse effect is not an aggrieved person under section 20 of the [Illinois Biometric Information Privacy Act]); but see Monroe v. Shutterfly, Case No. 16 C 10984 (Sep. 15, 2017)(declining to dismiss case based on plaintiff’s failure to allege damages).

Criminal Law: Biometric information challenges traditional concepts of privacy under traditional Constitutional jurisprudence. Consider for example, the plain view doctrine, which holds that evidence discovered in plain view during the course of a stop doesn’t violate the Fourth Amendment. But since certain biometric information -
such as facial recognition is always in plain view, does that mean that a police officer can snap a photo of a driver for speeding and run it through a database? Or does the fact that biometric evidence is non-invasive entitle law enforcement to collect a wide range of information whenever a suspect is arrested?

In *Maryland v. King*, 133 S. Ct. 1958 (2013), the Supreme Court, in a 5-4 decision ruled that "when officers make an arrest supported by probable cause to hold for a serious offense and bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment." The Court's ruling rested on both an arrestee’s reduced expectation of privacy, but also the minimal invasiveness of a DNA swab. Under this reasoning, an arrestee could be subject to a battery of biometric gathering procedures that while non-invasive to perform nonetheless unreasonably intrude on privacy because of the information produced. By contrast, Scalia, writing for the dissent held categorically that the Fourth Amendment categorically prohibits a suspicionless search - irrespective of how non-invasive it may be.

Biometric information implicates the Fifth Amendment as well. Whereas forcing an arrestee to disclose a password to a phone violates the right against self-incrimination, but compelling production of a fingerprint is sometimes viewed differently. See *State v. Baust*, 2014 WL 10355635 (Va. Cir. Ct. Oct. 28, 2014) (ruling that “the Defendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same,” because while the former is testimonial, “[t]he fingerprint, like a key, . . . does not require the witness to divulge anything through his mental processes”). But see *In re Application for a Search Warrant*, 236 F.Supp.3d 1066 (N.D. Ill. 2017)(granting search warrant for residence, but denying request "to compel any individual who is present at the subject premises at the time of the search to provide his fingerprints and/or thumbprints 'onto the Touch ID sensor of any Apple iPhone, iPad, or other Apple brand device in order to gain access to the contents of any such device). For additional discussion, see Erin M. Sales, Note, The “Biometric Revolution”: An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination, 69 U. Miami L. Rev. 193 (2014) (suggesting that “biometric authentication will not implicate the privilege to be free from self-incrimination”). But see Kara Goldman, Note, Biometric Passwords and the Privilege Against Self-Incrimination, 33 Cardozo Arts & Ent. L.J. 211 (2015) (“use of the fingerprint as a password is a direct link to communicative, as well as potentially incriminating, information, and serves as a replacement for traditional password, is protected by the Fifth Amendment.

*State Laws:* To date, three states - Illinois, Texas and Washington State have enacted laws to protect biometric
information. All three statutes prohibit the sale or disclosure of biometric information collected from an individual unless the individual consents to disclosure, or the disclosure is required by state or federal law or pursuant to subpoena. In addition, the Washington statute permits disclosure of biometric information without consent where doing so is necessary to provide a service subscribed to or authorized by the user. By contrast, Illinois’ Biometric Information Privacy Act (BIPA), 740 ILCS 14/5(b) also requires that a business in possession of biometric identifiers have a publicly available written policy, and to establish a retention schedule and guidelines for the destruction of biometric information. The policy must require the destruction of biometric information whenever the initial purpose for its collection has been satisfied, or within three years, whichever occurs first. Texas BIS has a one-year destruction period instead of three-year period, but does not require a publicly-available written policy.

Privacy Suits: Lawsuits have been filed against Facebook and Google under Illinois’ BIPA, alleging that the companies violated the law by collecting images from users without consent and using them to build “the world’s largest privately held database of consumer biometric data.” See Facebook Biometric Info. Privacy Litig, 185 F.Supp. 3d 1155 (N.D. Ca. 2016), Rivera v. Google, Inc., No. 16-02714 (N.D. Ill. Feb. 27, 2017) See Tech Companies Pushing Back on Biometrics, Bloomberg (7/20/2017). In Rivera, Google attempted to argue that its collection of facial images were not “biometric information” within the meaning of BIPA - a claim that the court quickly disposed of given BIPA’s broad definition of biometric information. The court also rejected Google’s claim that BIPA had extraterritorial effect; the court found that the Legislature had not intended extraterritorial scope and in any event, the acts took place in the cloud with, which sufficient local contacts could be presumed to be in Illinois. Facebook sought dismissal on other grounds - arguing that the plaintiffs not suffered harm and lacked standing under Spokeo. The judge rejected that argument, explaining that “The right to say no is a valuable commodity...The case concerns the “most personal aspects of your life: your face, your fingers, who you are to the world.” See Facebook Judge Frowns on Bid to Toss Biometric Suit, Bloomberg (11/30/2017)(discussing motion to dismiss). Both suits are considered bellweather cases and will be closely watched as they move forward,

Choice of Law: At least one court determined that Illinois substantive law would apply to a suit brought against Facebook under the BIPA and transferred to federal court in California. Although Facebook’s terms of use stated that California law should apply, the court declined to enforce them, and ruled instead that BIPA would govern. The court reasoned that if it were to enforce the California choice-of-law clause over Illinois Biometric Privacy Act (“BIPA”), "the Illinois policy of protecting its citizens' privacy interests in their biometric data . . . would be written out of
existence" because California has "no law or policy equivalent to BIPA In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155 (N.D. Cal. 2016), But see Palomino v. Facebook, Case No. 16-cv-04239 (N.D. Ca. 2017)(enforcing California choice of law clause in suit filed under New Jersey consumer protection statute, finding that California has its own robust consumer protection statutes).

Employment: With the advent of scanners, microchips, lawsuits against employers for collection of biometric data have exploded. In the latter half of the year, roughly 30 lawsuits were filed against employers, alleging violations of Illinois’ BIPA. See Illinois Employers Flooded With Class Actions Stemming From Biometric Privacy Law, IllinoisPolicy.org (10/17/2017). Employers adopting biometric devices - such as scanners or microchips to track employees cannot force employees to submit to tracking based on religious objections. In US EEOC v. Consol. Energy, 4th Cir. (6/12/2017), the Fourth Circuit affirmed a jury verdict finding that an employer wrongfully refused to accommodate an employee who informed his supervisors that his religious beliefs (which he documented with a note from his pastor) prevented him from using the scanning system.

Future Trends & Opportunities: Biometrics is just in its nascency and will challenge current beliefs regarding the meaning of privacy, and the extent of an individual's right to be left alone. Applicable law governing biometrics will also change, as more states enact biometric privacy statutes or if Congress steps in to propose a federal law.
BITTORRENT LITIGATION

WHAT IS IT?
BitTorrent is a protocol for peer-to-peer file sharing over the Internet that supports transfer of large files like music and movies. As had been the case with Napster, BitTorrent is similarly used for downloads of movies and music in violation of copyright law. BitTorrent can be used to share any type of large files, it is most frequently used to unlawfully share copyrighted materials. But BitTorrent isn’t only used for unlawful purposes: gaming companies and websites like the Wayback Machine (which achieved earlier iterations of websites) use BitTorrent to facilitate sharing of large files with users. See http://www.makeuseof.com/tag/8-legal-uses-for-bittorrent-you’d-be-surprised/

WHY NOW?
Not surprisingly, BitTorrent downloads have spawned litigation over copyright infringement and piracy. Many BitTorrent infringement cases were filed by the content creators - ranging from film studios or frequently pornography companies. But BitTorrent also attracted copyright trolls, who filed mass lawsuits against hundreds of users in the hopes of extracting a settlement.

KEY LEGAL ISSUES:
Copyright Trolls - Sadly, the best known example a copyright troll was a law firm called Prenda Law. The firm filed thousands of questionable infringement suits and was later discovered to have acquired copyrights to pornographic films and created its own pornographic content which it uploaded to BitTorrent sites and then turned around sued for infringement. See http://copyright.nova.edu/bittorent/. Prenda’s operation worked like this: Prenda would file lawsuits against multiple parties en masse, then seek discovery against the ISP for users’ identities. Subsequently, Prenda’s lawyers would send defendants’ letters, and used extortionist tactics (such as threatening to expose a user for downloading porn) to extract quick settlements. Once this activity was discovered through attorneys representing defendants, the suits were dismissed, Prenda’s lawyers required to pay damages and were also the subject of bar complaints and criminal charges for fraud. See see Ingenuity 13 LLC v. Doe, No. 2:12-cv-8333-ODW(JCx), 2013 U.S. Dist. LEXIS 64564, at *6-9 (C.D. Cal. May 6, 2013 (sanctioning Prenda); see also Copyright Trolls Steele and Hansmeier Arrested, Ars Technica (12/2016).

Civil Procedure and Evidentiary Issues - BitTorrent raised a host of civil procedure and evidentiary questions. Because BitTorrent users are located all over the country, copyright holders have attempted to subject users from multiple states to personal jurisdiction in a single location by virtue of them participating in a “swarm,” i.e., a group of

Conspiracy Issues - In an effort to avoid personal jurisdiction and joinder issues, copyright trolls adopted a clever new tactic in which they sue only a “single defendant who is connected to an IP address located in the district in which the plaintiffs brought suit, but . . . [seek] discovery about other IP addresses belonging to computer users who are not joined as defendants,” which they plan to later join in the suit. In those cases, plaintiffs allege that additional IP addresses represent co-conspirators “who conspired to infringe the plaintiff’s copyright by downloading the same file through the BitTorrent system.” These allegations, however proved unsuccessful as the mere fact that the computers of BitTorrent users communicated with one another does not create a conspiracy among users. See Timothy B. Lee, Judge Rejects Copyright Trolls’ BitTorrent Conspiracy Theory, ARS TECHNICA (Apr. 1, 2012),

Future Trends & Opportunities: Although as of this writing, BitTorrent suits are still being filed, the numbers are down from the heydey of a few years ago. Services like Netflix and Hulu have made it easier to purchase streamed content at a low cost and streaming pirate sites along with tools such as Kodi boxes make accessing copyrighted materials at no cost easier than using BitTorrent and more difficult to get caught. More recently, copyright holders have also taken a different approach to get at infringers - typically by threatening advertisers who support piracy sites rather than through direct litigation. See Long Slow Decline of BitTorrent, Plagiarism Today. All of these developments signal that BitTorrent isn’t like to be a growing practice area in the years ahead.
BLOCKCHAIN TECHNOLOGY

WHAT IS IT?
When we hear the term blockchain, we automatically associate it with bitcoin. But blockchain is so much more. Not only does it serve as a platform for cryptocurrency transactions, but it can serve for a variety of other contractual transactions - which are the subject of this section (cryptocurrency, arguably the most advanced use of blockchain, is addressed in its own section). As one commenter described, a "smart contract" is essentially an "automated blockchain transaction" that carries out what it is programmed to do. See Why Lawyers Won’t Be Replaced by Smart Contracts, Above the Law (October 2017).

By way of background, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically. Once a transaction is entered, the records cannot be altered because they are linked (via a "hash") to every transaction that came before. Computational algorithms are used to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network. See Harvard Business Journal (1/2017), https://hbr.org/2017/01/the-truth-about-blockchain (See the sidebar “How Blockchain Works.”)

Because blockchain ledgers are digital and transparent, they are well suited to support contractual transactions. Blockchain transactions can be programmed to automatically trigger consequences in transactions between users

WHY NOW?
The popularity of blockchain for currency has had a ripple effect on other industries, which are now adopting blockchain for other purposes. Examples include:

Corporate Law - A new Delaware law passed in August 2017 explicitly authorizes the use of distributed ledger technology in the administration of Delaware corporate records, including stock ledgers. See https://newmedialaw.proskauer.com/2017/08/02/delaware-authorizes-stocks-on-blockchain/ Currently stock ledgers are tracked on Excel spreadsheets which are prone to error. With ⅔ of the nation’s incorporations in Delaware, it is anticipated that this new law will quickly gain traction.

Energy industry: Blockchain can be used for solar power sales, energy trading and microgrids: See PowerTechnology.com (2016).

Real Estate and Property: Blockchain can facilitate property sales and rentals through self-executing and secure contracts (See Blockchain Could Change Everything in Real Estate, Venturebeat,
(11/18/2017) or provide a platform to convey title and register land records. (see Cook County Report on Pilot Blockchain Experiment (11/2016) (summarizing results of blockchain pilot program).

**Family Law:** In 2016, a couple uploaded a prenuptial agreement to Ethereum (a blockchain platform) See Pre-Nup Agreement at Ethereum, Coindesk.com (June 2016) and additional discussion at https://gaytonlaw.wordpress.com/tag/statute-of-frauds/).

**Healthcare:** Blockchain provides secure storage for medical records, while allowing patients to retain control instead of centralized companies. See https://cointelegraph.com/news/new-blockchain-Based-startups-create-new-opportunities-for-healthcare

**Music:** Blockchain will allow for peer-to-peer music exchanges (as with Napster) - but ensuring that artists get their fair share. Blockchain may also track digital ownership rights and help cut down on piracy. See https://thenextweb.com/contributors/2017/08/15/five-ways-blockchain-tech-going-rock-music-movie-industries/

**KEY LEGAL ISSUES:**

*Jurisdictional and choice of law issues:* where servers are decentralised and can be spread around the world, pinpointing where a breach or failure occurred (and taking the appropriate cross-border action) may be complex. See Legal Aspects of Blockchain Contracts, Virtual Currency Report (5/2017).

*Contract law:* Because a smart contract is self-executing (e.g., buyer agrees to have money taken from escrow for rent), a party seeking to challenge it is placed in a position of seeking relief after the contract is performed. Smart contracts also do not allow for ambiguity, so contract drafters may need to learn to reframe contractual language. There are also questions about how smart contracts will deal with modification. For extensive discussion of legal issues related to smart contracts. See Legality of Smart Contracts, Georgetown Law Review (4/2017).

**Law and Technology Mismatch** - For some applications, law may not have kept pace with blockchain technology and may necessitate new legislation - as in the case of corporate record-keeping in Delaware. Similar changes may be required for other industry-specific blockchain applications.

**Varying state laws:** In many instances, state law will govern validity of blockchain (as in Delaware) even though transaction may take place across state lines. For example, are blockchain transactions enforceable in all jurisdictions. Arizona recently passing a law that deems electronic transactions enforceable but what about other states? What if a consumer enters into a smart contract and later needs to seek enforcement beyond self-execution - only to have a state court deem the contract void on policy grounds or unenforceable due to electronic format?

**Blockchain & the SEC** In recent months, several public companies -- like LongIsland Iced Tea have added “the term “blockchain” to their names (now LongBlockchain which has lead to Huge increases in valuation (LongIsland Iced Tea stock spiked 500%). The SEC recently issued a warning of its intent to crack down on companies that convert their businesses overnight to brand themselves as blockchain companies because it’s difficult to
determine which names reflect legitimate businesses rather than companies trying to hype their stock, reports Tech Crunch.

**Update: Legal Ethics & Bitcoin**

New York lawyers may face a potential twist when it comes to holding bitcoin for clients in trust according to Devika Kewalramani writing at the New York Law Journal. A recently-adopted New York virtual currency law, N.Y. Comp. Codes R. & Regs. tit. 23, § 200 (2015) requires a person “storing, holding, or maintaining custody or control of Virtual Currency on behalf of others” to obtain a Bitlicense. The regulations do not contain any exceptions for bitcoin held in a lawyer trust account, meaning that New York lawyers could be subject to this requirement if they were to deposit bitcoin payments into a trust account.

**Future Trends & Opportunities:**

A recent article by Caitlin Moon in Law Technology Today (January 2017) described multiple opportunities for lawyers in blockchain moving forward, including (1) creation of a smart title company that relies on blockchain technology to transfer title, (2) advising on blockchain law specific to a niche, (3) specializing in Smart Contract drafting and mediation which may involve a different skill set than traditional contracts (which may have too much ambiguity) and (4) protecting vulnerable consumers from fraud and overreaching in blockchain contracts.
WHAT IS IT?

Campus defense law encompasses lawsuits that occur on college campuses specifically related to harassment and assault, which are considered a form of discrimination under Title IX. Title IX prohibits any educational program receiving federal funds from excluding from participation or discriminating against any person on the basis of sex. To avoid loss of funding under Title IX, most universities established disciplinary codes and hearing boards to respond to charges of sexual harassment and assault. Increasingly, both the complainant and the accused retain counsel in these proceedings, which are often highly publicized and contentious.

WHY NOW?

Over the past fifteen years, charges of sexual assault and harassment have captured increased attention in the media with recent accusations against public figures like Harvey Weinstein and Roy Moore. A recent federal study found that reports of sexual assaults on college campuses increased 205 percent between 2001 and 2014.

Meanwhile, federal policies governing victims’ rights have changed with each administration. Under the Obama Administration, colleges receiving federal money were advised to use the lowest possible standard of proof (a preponderance of evidence) in sexual assault cases; allow accusers to appeal not-guilty findings; accelerate adjudications with a recommended 60-day limit; and, strongly discouraged cross-examination of accusers. The Trump Administration rolled back many of these guidelines to afford more protection to the accused by requiring schools to apply a higher standard of proof and provide the accused notice and sufficient time to prepare for interviews and an opportunity to cross examine opponents.

In 2014, the DoED issued new guidelines that included transgender student protections under sexual discrimination. Again, it is unclear whether these guidelines will continue to apply under the new Administration.

KEY LEGAL ISSUES:

Lack of Process for accused The biggest complaint of the Title IX guidelines has been that the schools are in charge of the “investigation, prosecution, fact-finding, and appellate review,” and it has become a kangaroo court. At least two federal courts have denied colleges’ motion to dismiss in lawsuits by accusers challenging lack of due process. See Sterrett v. Cowan, Case No: 2:14-cv-11619 (E.D. Mich. 2015), John Doe v. Brandeis Univ., 177 F. Supp. 3d 561(D. Mass. March 31, 2016),
Discrimination Against Accused - In Doe v. Columbia Univ., 831 F.3d 46 (2d Cir. July 29, 2016), reversed the lower court's ruling to dismiss plaintiff's claim, permitting a claim under Title IX when the school exhibited anti-male bias for suspending the accused for a year for an assault claim; the school settled the case on July 17, 2017. Most recently, the Sixth Circuit, in Doe v. Univ. of Cincinnati, 2017 U.S. App. LEXIS 18458 (6th Cir. Sept. 25, 2017), upheld the lower court's decision to block suspension of a graduate student, holding that the university did not respect his constitutional rights after he was accused of sexual assault.

Transgender Issues A federal district court granted injunctive relief to a transgender student G.G., directing the school district to permit the student to use the bathroom according to his gender-identity (id., 2016 U.S. Dist. LEXIS 93164 (E.D. Va. June 23, 2016). The Supreme Court granted cert of the ruling. 136 S. Ct. 2442 (Aug. 3, 2016), cert. granted, 137 S. Ct. 369 (Oct. 28, 2016)).

Defamation - The Second Circuit revived the defamation claims over a Rolling Stone article on campus rape, reversing and remanding the decision back to the trial court. See Elias v. Rolling Stone LLC, No. 16-2465, 2017 U.S. App. LEXIS 18252 (2d Cir. Sept. 19, 2017); 2017 U.S. App. LEXIS 18686 (2d Cir. Sept. 22, 2017) (full opinion). In another case involving Columbia University and her (referred to as "Mattress girl"), the accused student sued Columbia for defamation of lack of fair process in its investigation of the incident.

Failure to protect or retaliation A Title IX civil lawsuit can be filed in federal court. The victim-complainant can sue the educational institution and prove the school knew or should have known about the sexual assault or harassment of a student, or subsequent retaliation against the student, and did not investigate or handle the situation properly. It is notable that Title IX has no express limitations period; consequently, some courts have fashioned the applicable statute of limitations based upon state law claims (see, e.g., Jane Does 1–10 v. Baylor Univ., Case No. 6:16-CV-173-RP (W.D. Tex. March 7, 2017) (applying two-year general personal injury statute of limitations period under Texas law to the Title IX claim). Alternatively, the accused-complainant can sue the educational institution for constitutional right violations, negligence and/or breach of contract for failure to properly evaluate allegations and/or remedies imposed upon the accused student.
Future Trends & Opportunities:

In light of recent allegations against public figures and corresponding movements (symbolized by the popular hashtags #MeToo, #RoseArmy, #HowIWillChange, #BeBrave, #Honesty, #StartACircle, and #LeanIn), society may be facing a pivotal transformation in the fight against sexual assault and harassment against women in general. Thus, we can expect more aggressive campaigns against discrimination to emerge everywhere (See Cyberbullying Chapter), not just college campuses. At the same time, recent changes in the Administration’s guidance on Title IX may make proof of discrimination or assault more difficult in campus disciplinary proceedings.
WHAT IS IT?

Cannabis - also known as marijuana, pot and other names - is a psychoactive drug from the cannabis plant used for recreational or medical purposes. Cannabis law encompasses the range of issues related to the legalization of marijuana for medical and recreational use - from criminal defense for possession and distribution to the tax and corporate issues related to establishing marijuana dispensaries. See Wikipedia, Cannabis. Many of the complexities related to Cannabis Law arise as a result of a conflict between state laws legalizing use and federal law which continues to treat cannabis as an illegal Schedule I drug. See 28 U.S.C. § 214(c), Schedule I(c)(10) (2015). There are also many different players in the cannabis “food chain” - medical dispensaries, growers and cultivators (which may differ if growing for medical or recreational marijuana), retailers, manufacturers and testing facilities - each subject to its own unique set of licensing or business registration requirements. See Marijuana Laws State by State (Findlaw)

WHY NOW?

Whereas 15 years ago, only a handful of states had laws legalizing marijuana for medical use by qualified patients, today, 29 states and the District of Columbia have laws broadly authorizing medical marijuana (including establishment of medical dispensaries). Of those states, eight have also legalized marijuana for recreational use, beginning with Washington State and Colorado in 2012. State efforts were complemented by two federal initiatives designed to prevent federal enforcement of the Controlled Substance Act in states where cannabis is legalized. See Rohrabacher-Farr Amendment (prohibiting the United States Department of Justice from spending federal funds to interfere with the implementation of state cannabis laws - but must be re-enacted each fiscal year) and 2013 Cole Amendment, (advising prosecutors to de-prioritize federal drug enforcement efforts in states where cannabis is legal). With a new Administration and Republican Congress, the future of these policies is currently under examination - though the uncertainty has not slowed the cannabis industry yet. In 2017, cannabis sales grew by 33% to end 2017 with $9.7 billion in sales according BDS analytics, and with California, Maine and
Massachusetts all scheduled to open recreational use markets in 2018, growth is expected to continue.

**KEY LEGAL ISSUES:**

**State v. Federal Criminalization Status** - Although legal in many states, marijuana remains a controlled substance for criminal purposes. Under the Obama Administration, prosecution of marijuana crimes under federal law was de-prioritized in jurisdictions where marijuana is legal per the Department of Justice Cole Memo of 2013 - thus giving some comfort to legal marijuana businesses (and their investors) that they would be free of interference by the federal government. That policy changed overnight on January 4, 2018 with the issuance of the Sessions Memo which instructs prosecutors to enforce and prosecute the Controlled Substances Act as related to marijuana activities, irrespective of its status under state law. As a result of the memo, marijuana stocks plunged as a result of the present uncertainty as to whether a wave of criminal prosecutions may follow.

**Corporate Entity** For businesses engaged in the cannabis industry, even an activity as mundane as corporate entity selection can be tricky. Laws on acceptable corporate structures vary from state to state - in some jurisdictions, for example medical dispensaries must be organized as non-profit or benefits corporations, while in others, a certain form of business entity may be required (or alternatively, unavailable) for a particular function - e.g., retail, manufacturing, etc...As states transition to legalization, legacy entities - such as “collectives” (an entity used in many states pre-legalization to operate medical dispensaries and avoid federal penalties) are being phased out, with companies needing advice on when to transition to a new corporate structure and which to choose. See California Cannabis Licensing and Collective Model, Canna-Law Blog, 11/2017)(discussing considerations in moving away from collective model). Sometimes tax considerations dictate entity form. For example, although LLCs are popular with startups, LLC members are personally responsible for tax liability. Given the potential for audits under Section 280e of the IRC (see below), some tax advisors recommend a C-corporation since shareholders are insulated from the corporation’s tax liability. See Corporate Legal Structure Cannabis, FutureCannabisProject.com, 2/2016. Finally, B-corporation status (See Social Entrepreneurship) for marijuana businesses is not available at this time due to varying state laws on legalization and federal criminalization.

**Tax Law** - Cannabis businesses face a significant disadvantage tax wise that ordinary businesses do not. Because marijuana is a Schedule I substance under federal law, cannabis businesses - though fully legal under state law - cannot deduct ordinary business expenses (e.g., rent, salaries, advertising, etc..) under Section 280e of the Internal Revenue Code, though they can deduct cost of goods sold. See 2015 IRS Memo Re: COGS for illegal substances. The
Ninth Circuit recently rejected a challenge to Section 280e, alleging that as applied, it resulted in excessive fines in violation of the Eighth Amendment. See Canna Care v. IRS, No. 16-70265 (9th Cir. July 2017).

**FinCen Guidelines & Banking** Not surprisingly, banks have been reluctant to serve cannabis companies for fear that they could face audits or charges for money laundering under the Controlled Substance Act. In 2014, the Department of Justice released a memo assuring financial institutions serving marijuana businesses in compliance with state law that they were low priority for enforcement action. That same year, Financial Crimes Enforcement Network issued guidelines under which banks can provide financial services to marijuana business without violating federal law. Even with these changes, many marijuana businesses find it difficult to find banking services, and operate as purely cash businesses, reports the LA Times (12/14/2017) - something that California is now seeking to change by putting in place measures to encourage the marijuana industry to go cashless.

Trademark Cannabis businesses face another disadvantage arising out of federal criminalization: inability to register for federal trademark protection. The USPTO Trademark Manual of Examining Procedure (TMEP) Section 907 explains that under Trademark Rule of Practice 2.69, “[u]se of a mark in commerce must be lawful use to be the basis for federal registration of the mark, with no exception even for marijuana for medical use.clarifies that federal law does not even provide no exception to the above-referenced provisions for marijuana for ‘medical use.’” See M.Trudell, Marijuana: Some States Let You Smoke It But You Can’t Register a Trademark for It, INTA (Aug. 2015), citing USPTO Manual. The USPTO trademark prohibition applies to businesses that sell or produce any cannabis products that are illegal under the Controlled Substance Act. Even if the proposed trademark does not mention the work “cannabis” or “marijuana,” the USPTO can look at external sources like a company’s website to determine whether the trademark is sought in connection with a lawful business. See In Re Morgan Brown Serial No. 86362968 (July 14, 2016)(denying trademark protection to HERBAL ACCESS after discovering through application and company website that business will sell marijuana in addition to other herbal remedies). On the other hand, companies can seek trademark protection for a cannabis or marijuana brand for ancillary products, like t-shirts or apps. See e.g., Marijuana Trademarks & Branding Cannabis Products (April 18, 2017) (describing USPTO finding that TOKR trademark for app that lists marijuana dispensaries does not violate CSA and therefore complies with “lawful use” rule.); also Marijuana Trademarks, LA Times, 1/4/2017)(examples of brands like “Hi” trademarked for T-shirt and other ancillary cannabis businesses).

Because USPTO’s lawful use rule is tied to CSA compliance, changes in federal substance control policy can result in revision of
USPTO policies. For example, up until recently, USPTO approved trademarks for products containing CBD, a hemp extract available nationwide. However, a recent change in the Drug Enforcement Agency’s classification of CBD lead the USPTO to reverse course, and at least for now, treats trademarks for products containing CBD (even lotions with trace amounts of CBD) as violating the lawful use rule. See USPTO New Stance on Cannabidiol, Cannabis Business Times (Dec. 2017).

**Organic Certification** - Organic Certification + Cannabis - USDA organic certification is not available for cannabis because it is a controlled substance - though recently, USDA made an exception and offers organic certification for industrial hemp produced in compliance with applicable state law. See USDA Regulation re: Hemp, Federal Register, 8/12/20160; See also Section on Organic Certification.

**Bankruptcy** Because cannabis related businesses violate federal law, they do not qualify for relief under the bankruptcy code. See e.g., In re: Arenas, 535 B.R. 845 (10th Cir. BAP 2015)(dismissing bankruptcy petition filed by state-licensed marijuana grower and wife under Section 7 because Trustee would violate federal law by administering assets, and denying conversion to Section 13 since debtor plan would be funded by illegal activity); In Re McGinnis, 453 B.R. 770 (Bankr. D. Or. 2011) (holding that a chapter 13 plan was unconfirmable because it relied on a future change to Oregon medical marijuana law and it violated federal law)Even lawful businesses that knowingly lease space to marijuana businesses violate the CSA and cannot seek bankruptcy relief. Rent Rite, 484 B.R. 799, 805 (Bank. D. Colo. 2012). As if the caselaw was not sufficiently clear, in December 2017, two DOJ officials issued a reminder that the bankruptcy system cannot aid in liquidating or restructuring any assets associated with cannabis. See No Bankruptcy for Marijuana Businesses, Forbes, 12/05/2017.

**Advertising** - States each have their own set of regulations on advertising for medical marijuana dispensaries and recreational marijuana sellers. See State by State Guide to Cannabis Advertising online at leafly.com; also Can Puff the Magic Dragon Lawfully Sell His Wares, Judy Endean, ABABar.org (Summer 2015)(detailing different state regulations).

**Rico Claims** The Racketeer Influenced and Corrupt Organizations (RICO) Act allows individual parties to recover civil penalties for racketeering activity performed as part of a criminal enterprise. A recent 10th Circuit case ruled that property owners harmed by noise and owners stemming from an adjacent marijuana growing business operating lawfully under state law could bring a RICO claim in connection with the activity. See Safe Streets v. Hickenlooper, No. 16-1048 (10th Cir. June 7, 2017). The Tenth Circuit found, fairly easily, that operating a cultivation facility constituted “racketeering activity” within the meaning of RICO because it involves “dealing
with a controlled substance.” The court next found that the growers pooled their resources with other growing facilities to achieve enterprise efficiencies, and therefore were an enterprise activity. Finally, the court found that the plaintiffs’ alleged harms from the operation of a “criminal enterprise” - such as odor that diminished property value - established standing to sue. **Needless to say, the Safe Streets precedent may create added risks for the cannabis industry because it has the potential to transform garden variety nuisance claims into a federal case.** But see *Qullinan v. Ainsworth*, Case No. 4:17-077 (October 5, 2017)(dismissing RICO claim against marijuana business that purchased warehouse and subsequently evicted month to month storage unit tenants, finding that harm to evicted tenants resulted from termination of lease and not unlawful cannabis activity).

**Future Trends & Opportunities:** As more states legalize cannabis either for medical or recreational purposes, opportunities will abound. Moreover, with the law in flux, the need for attorneys well versed in legal precedent and policy will be in high demand for years to come.
BONUS FOR LAWYERS: Ethics of Representing Cannabis Clients

Lawyers are prohibited from counseling a client to engage in conduct known to be criminal. See Model Rule 1.2(d) of Professional Conduct. Because federal law criminalizes cannabis, lawyers representing cannabis businesses would run afoul of Model Rule 1.2(d), even if marijuana is legalized in the jurisdictions where they practice. To resolve this tension, several states have amended their version of Model Rule 1.2 to allow attorneys to counsel clients on activities that are lawful under state and federal law. See Legal Ethics of Advising Cannabis Clients, Wilson Elsner (September 2017)(summarizing state ethics codes regarding representation of cannabis clients). Many states also require lawyers to explain to cannabis clients that marijuana remains an illegal controlled substance under federal law, potentially exposing them to criminal liability even if fully compliant with state law. That said, some commenters have suggested that representation of cannabis clients could result in loss of attorney-client privilege (since communications in furtherance of criminal activity are not protected) or loss of malpractice coverage (which ordinarily does not cover criminal activity). See Bruce Reinhart, Legal and Ethical Pitfalls in Marijuana Law, ABA Criminal Justice (Winter 2017).
CLIMATE CHANGE LITIGATION

WHAT IS IT?
Given that climate change is the greatest environmental challenge of our time, it is unsurprising that it is increasingly becoming a subject of litigation. Litigation over climate change usually takes one of two forms: (1) administrative law litigation, which seeks either to force government regulators to take action on climate change, or to prevent them from doing so; and (2) common law litigation, which seeks to enjoin pollution based on a nuisance theory.

WHY NOW?
Although scientists and politicians have known for decades that greenhouse gas emissions may alter the climate, the science has become unequivocal in the past 20 years. Congress’ failure to take meaningful action to address the problem (Congress last updated the Clean Air Act in 1990) has lead organizations concerned about climate change to turn to the judiciary. It is expected that under the Trump Administration, many environmental policies and programs will be rolled back - which may give rise to administrative challenges - or heighten the need for private climate change litigation as an alternative.

KEY LEGAL ISSUES:
Environmental litigants have had some success in pursuing administrative law remedies. In the landmark case of Massachusetts v. EPA, the Supreme Court held that EPA had authority to regulate carbon dioxide and other greenhouse gases under the Clean Air Act. EPA responded by moving to regulate emissions from cars and trucks. In 2010, the U.S. House of Representatives passed the American Clean Energy and Security Act (commonly known as “Waxman-Markey”), a bill that would have created a cap-and-trade system to reduce greenhouse gas emissions. When that bill failed to pass the Senate, the Obama Administration used its authority under the Clean Air Act to implement a variety of regulations aimed at reducing emissions from power plants and other industrial sources. Industry groups and conservative states (lead by Scott Pruitt, then Attorney General for Oklahoma) challenged these rules. Many of these challenges were pending when Donald Trump took office. Trump appointed Scott Pruitt to serve as the new EPA Administrator, and Pruitt quickly moved to repeal the Obama-era climate rules. That has lead environmental groups to sue, seeking to preserve existing regulations. These groups have scored at least one early success.

Parallel to this administrative law litigation, litigants have also brought nuisance actions against significant polluters. So far, this strategy has not been successful. In AEP v. Connecticut, the Supreme Court unanimously rejected Connecticut’s argument that the federal common law of nuisance provided a remedy to states threatened by climate change. Climate change litigation by private
parties has met with mixed success. In *Juliana v. United States*, Case No. 6:15-cv-01517-TC (D. Or. 2015), the court denied a motion to dismiss a suit filed by a small group of young people and a climate scientist representing future generations are suing the federal government for violating their asserted constitutional rights to a stable climate system. But courts have dismissed other cases where litigants pursued state common law claims to remedy climate change harms—sometimes finding that the proper response to climate change is a political question, and finding that the plaintiffs lack standing. Some litigants are finding more success with climate change litigation in courts overseas. See Emerging Trends in Climate Change Litigation, Law 360, online at https://www.law360.com/articles/766214/emerging-trends-in-climate-change-litigation.

**Future Opportunities & Trends:** We are likely to see continued litigation in this area until the political branches adopt a comprehensive plan for mitigating climate change. The most impactful litigation will be in the administrative arena, with litigants seeking to force EPA to regulate GHGs or to prevent it from doing so. Some litigants may also pursue common law theories, but these cases are unlikely to succeed.
WHAT IS IT?

Coworking law is a catchall for the unique legal issues spawned by the increasing popularity of co-working spaces. Co-working spaces are defined as membership-based workspaces where diverse groups of professionals work together in a shared, communal office facility. Coworking has two variants - hoteling - an office without assigned desks/offices, instead offering a reservation-based style where employees schedule for workspaces on an as-needed basis and coworkation, which caters to location-independent professionals referred to as “digital nomads” that travel from one space to another all over the globe (think short-term ex-pat).

Co-working law encompasses the unique legal issues - from real estate and insurance to discrimination - that emerge as coworking increases in popularity - with a need for legal services both to facilities that seek to offer coworking space, and tenants who use the space. Co-working spaces for lawyers also raise unique ethics issues.

WHY NOW?

Following the global financial crisis of 2008-2009, there was a boom of co-working spaces throughout the country, especially in large and mid-size cities due to the evolving nature of work in the modern world. Today, co-working spaces are not just for freelancers and solo-preneurs; companies may lease space for telecommuters or set up shop within a coworking space. The statistics confirm the trend: In 2014, Inc. Magazine reported there was 83% growth in the number of co-working spaces, with memberships increasing by 117% between 2012 and 2013.

KEY LEGAL ISSUES:

Building Ownership - A tenant is granted exclusive rights to a defined space in a commercial building, together with legal protections against eviction. Members of a co-working space are not afforded these same types of protections, and the fact is smaller, local co-working businesses come and go, leaving their members “officeless.” Members must recognize that the building owner may be a separate entity from the co-working company, and should ask to review the lease. By way of example, in 2014, Hudson Pacific Properties (HPP) sued Real Office Centers (ROC) for unpermitted use of a terrace (which was considered a landmark of big parties in the region’s booming tech industry over the last 5 years), and the parties settled with a new 10-year lease in place, but without the revenue from the terrace parties, together with the cost to remedy building violations (like an unpermitted audio-recording studio and ADA non-compliant bathrooms), ROC could not pay its rent and
HPP filed for eviction in May 2017. See also, e.g., Frick Lender Assocs. v. Coterie (Ct. Com. Pl., Allegheny Co.), a lawsuit filed on July 7, 2017, seeking $220,000.00 in past-due rent and eviction of the woman’s only co-working space from downtown Pittsburgh.

**Insurance** - An employee enjoys many insurance benefits through its employer, such as office coverage, E&O coverage, cyber liability and worker’s compensation. Similar to the landlord-tenant eviction protections, a landlord would have liability insurance for personal injury and property damage to a tenant; however, these protections are not necessarily in place in a co-working space. A co-working member must make sure that his/her equipment is covered from physical or cyber theft, and should check that the co-working company has adequate liability insurance or if separate insurance should be maintained.

**Data Security & Privacy** - Co-working members must take reasonable steps to ensure cyber security and encryption features are used to protect the transfer of online data, which security features may not be offered through the co-working space. In addition, there are concerns with ensuring privacy protections of personal client information.

**Alcohol Use** - Co-working spaces are designed to be relaxed, inspiring and fun, and many offer alcohol as a perk (or beer pong for recreation rooms). However, there is no employer to enforce the appropriate time and/or amount of alcohol use; discipline anyone for excessive alcohol use; or mediate the uncomfortable situations that can follow (especially for those in a combined living/co-working space).

**Sexual Harassment or Discrimination:** Because co-working business are not employers of its members (as opposed to its role as an employer for those who run the business), there is currently no set obligation or legal responsibilities to supervise, investigate and discipline its members for any unwelcome harassing or retaliatory behavior. Nevertheless, it is recommended that co-working spaces have and enforce sexual harassment policies.

**Miscellaneous:** Coworking facilities also give rise to the sorts of run of the mill business issues encountered by any office facility. As mentioned in the ROC and Coterie cases, supra, there are landlord-tenant disputes between the businesses and building owners. In Austin, Texas, co-working space Capital Factory is claiming trademark infringement and poaching of employees and customers against the newly formed atx Factory. See Cap. Factory Mgmt., LLC v. ATX Factory, LLC, Case No.: 1:17-cv-00797-LY (W.D. Tx.) filed on August 16, 2017.

**Future Trends & Opportunities:** As workers are much more transient, co-working spaces are a natural development to balance human interaction with the online work world. As co-working spaces grow further and begin offering benefits to users of the space, issues will continue to evolve.
**Bonus: Coworking And Ethics Considerations For Lawyers:** Co-working spaces for lawyers may raise unique ethics considerations. There are some companies tailored to attorney-only co-working spaces, and, even, local bar associations are offering spaces to new attorneys, solo practitioners and small firms to conduct work away from home. However, lawyers must be cognizant to take extra precautions to prevent any potential problems.

Confidentiality (Model Rule 1.6): Lawyers must ensure client confidentiality by separating client files as well as taking care that the emails and any communications with the client are solely between attorney and client. While there is an open layout, and trusting, collaborative spirit to the whole co-working paradigm, lawyers must be able to speak in person or on the phone with their clients in a private, quiet place (which also safeguards the attorney-client privilege, especially in terms of litigation or other court matters). It may be an overlooked privilege, but attorneys typically enjoy being able to leave their confidential documents or written communications when moving about their law firm; this evaporates in the co-working space. A lawyer cannot leave confidential information accessible, and concerns are, for example: documents on the table or open on the computer when unattended (even when just getting a coffee); using the wireless printing station (can someone else take it or reprint it?) or accidentally leaving pages behind in the printing station; using the shared fax system (should be using electronic fax services); or the security of the shared wireless network in sending and receiving emails.

Conflicts of Interest (Model Rule 1.7): It is imperative to know the other business (and lawyers) in one’s co-working space, to avoid any potential conflicts of interest or the appearance of impropriety. What if you are unknowingly talking to opposing counsel? What if you are listening to a co-working member’s story, and somehow learn inside information to one of your established cases or, possibly, a future case (and thereby, prohibited from representing future client).

Fee Splitting and Referrals with Lawyers and Non-Lawyers (Model Rules 1.5 and 5.4): For attorneys, networking and referrals through a co-working space can be considerable; attorneys benefit greatly from mixing with their co-workers (whether other attorneys or not). However, expectations of referrals must be clearly delineated and any fee splitting arrangements must be in writing, and clients must be informed.

Partnership or Not (Model Rule 7.2 and 7.5): A lawyer cannot state or imply that they practice in a partnership or other organization unless it is a fact. Co-workers are simply not associates or partners. References to your co-working space or other lawyer members in your space on your website, in ads or blogs may imply connections or associations in violation of these rules. Conversely, if you are so associated or connected with other lawyers (or ethically connected with non-lawyers), clients need to be informed in writing of the same.

Safekeeping Fiduciary Duties (Model Rule 1.15): As a lawyer in an open space that is filled with other members, one must ensure that clients’ property (especially money) is secure, and not accessible to others.

Bonafide Office Space Requirements - Some states still have bonafide office requirements (See Lawyerist at [https://lawyerist.com/states-require-bona-fide-office/](https://lawyerist.com/states-require-bona-fide-office/) listing each state’s requirements) and depending upon jurisdiction, coworking spaces may or may not comply. Lawyers who intend to use coworking space as primary space should consult the their local ethics rules.
CRAFT ALCOHOL

WHAT IS IT?

The term “craft” as applied to beer, spirits, cider and wine (collectively referenced as craft alcohol) is generally understood to refer to a product that is produced in small quantities by small independent or home-based breweries or distilleries that employ high-quality, natural and local resources in production. See e.g., Brewers Association (definition characteristics of craft beer), American Distillers Institute. Because of the heavily regulated nature of the alcohol industry, the legal issues applicable to craft beer, wine or spirits are wide-ranging -- from ordinary business issues (such as incorporation or trademark) to those unique to sale, advertising and regulation of alcohol.

WHY NOW?

In large part, the demand for craft beer and distilleries has been fueled by the growing trend of buying local. Social media -- which may be used by the craft beer and spirits industry, subject to some restrictions -- (e.g., ensuring that platform is primarily used by adults) has also enabled local companies to cultivate loyal fans who eagerly to share their discovery of a new brand with their friends. Other sources claim that increased interest in craft beverages flows from pop culture with shows like Mad Men reviving interest in bourbon. The numbers confirm that craft industries are on an upward trajectory: in 2016, the retail dollar value of the craft beer market was estimated at $23.5 billion and accounts for nearly 22 percent of the overall beer market, according to the Brewers' Association. Fortune reports that craft distilleries are the next big thing, with $2.4 billion in retail sales in 2015 and commanding 2.2% of the market, up from just .8 percent in 2010.

KEY LEGAL ISSUES:

Corporate Issues - Like any businesses, craft alcohol producers or sellers must deal with the same kinds of issues as any other business: corporate formation, zoning law, IP protection and taxation. Two issues warrant special mention: trade secret protection, which has become a source of concern and litigation as the industry becomes more competitive and b-corporation status (See Social Entrepreneurship) which has gained popularity with many craft companies that are often operated as sustainable and social-minded enterprises. See e.g., B-Corporation-net (listing 88 craft beer companies as b-corporations).
Insurance Considerations - Craft alcohol facilities like taprooms or distilleries face unique liability concerns related to production (such as long-term distilling periods) and liquor liability. Generally, policies can be crafted (pun intended!) at price points appropriate for a small tasting room to a popular and well-trafficked taproom.

Three-Tier Regulation - Following Prohibition, many states adopted a three-tier regulation system for alcohol sales under which producers can sell their products only to wholesale distributors who then sell to retailers, and only retailers may sell to consumers. Producers include brewers, wine-makers, distillers and importers. See Wikipedia. Three-tier regulation is particularly onerous for small craft producers who are often not large enough to attract wholesale distributors and would prefer to sell directly to the public. Thus, some states have adopted an exception for brewpubs, defined as establishments like microbreweries that produce and sell beer on site and as such, are not required to sell to a wholesaler. In other jurisdictions, there may be ways to structure contracts to bypass the three-tier restrictions. Other laws specific to the craft beer industry can be found at the Brewers Association website.

Labelling Litigation - Many companies have attempted to capitalize on the popularity of the craft trend by using the term as part of their labelling. This practice has spawned a number of lawsuits, summarized at here at the BevLawBlog.com. One of the most notable cases in this category is Parent v. Miller Coors, 3:15-cv-1204, where a consumer brought a class action against MillerCoors, claiming that the Coors’s labelling and marketing of its BlueMoon Beer as a craft beer is deceptive and misleading because the beer because the beer is manufactured by a large company and would not qualify as a craft beer under the Brewers Association Guidelines. The court dismissed the case, finding first that the Coors protected under the Safe Harbor Doctrine, which holds a defendant cannot be liable for a violation of consumer protection statutes if the business practice is permitted by another regulation. Here, Coors was subject to detailed federal and state labelling regulations neither of which prohibited Coors from using the name “Blue Moon” on its label. The court also found that the phrase “artfully crafted,” which is used on the Blue Moon label is not misleading because it is difficult to see how the phrase could reasonably be interpreted as a statement of objective fact. Other courts have disposed of these claims on similar grounds.

Craft Beer Certification - The “craft” designation is critical because craft beer and spirits are generally more expensive than mass-produced products. However, consumers will pay a premium for authentic craft products. In an effort to avoid dilution of the term “craft,” industry groups like the Brewers Association and the American Distillers Association have introduced certification programs that allow qualifying companies to hold themselves out as certified craft beer or spirits in their advertising. But as an industry
group, the Brewers’ Association lacks the power to enforce its certification requirements (e.g., by issuing a penalty or cease and desist against a company that calls itself a craft product) is limited. Thus, companies may require more than a trade group certification to protect the use of the term “craft.” See Kellie Money, Certifying Craft: Preserving Authenticity in the Craft Beer Market, 55 U. Louisville L. Rev. 413 (2017) (exploring different approaches to ensuring authenticity of craft designation).

Advertising: Advertising by craft breweries and distilleries is subject to federal Alcohol and Tobacco Trade Bureau requirements (see TTB Regulations - generally governing certain disclosures) and voluntary guidelines adopted by industry trade associations that are periodically reviewed and enforced by the FTC. See FTC Guidance (restricting companies from advertising on sites geared to under-21 audiences). States also have their own laws, though some - like California and Michigan have relaxed requirements for social media advertising, for example, by allowing retailers to interact with customers online or to list where the product can be purchased.

Future Trends & Opportunities:

The craft alcohol industry is booming, with existing craft breweries and distilleries growing, new craft products (like ciders and fruit wines) emerging. Because of the favorable impacts that the craft industry has on local economies, many states are re-examining their current laws to encourage the craft industry. In short, the craft alcohol industry will provide many opportunities for lawyers in every state with an interest in this practice area.
CROWDFUNDING

WHAT IS IT?
Crowdfunding law describes those legal issues that arise out of crowdfunding, which is a form of project funding accomplished through raising many small amounts of money from a large number of people (i.e., a crowd), typically via the Internet. Traditional crowdfunding sites make money by gathering pre-orders for products under development, or accepting donations in exchange for a gift. Crowdfunding has been used to raise money for a wide variety of commercial projects - from restaurants to books and documentaries to product inventions (which frequently solicit funding on Kickstarter and Indigogo) as well as are also sites to raise funds for charities and non-profits (e.g., NetworkForGood and Razoo). GoFundMe is a site where anyone can raise money for personal causes - including money for lawsuits or even to start a law firm. According to Wikipedia, it was estimated that in 2015, crowdfunding raised over $34 billion worldwide.

WHY NOW?
Crowdfunding is expected to surge in popularity in the coming years for two reasons. First, new technology is driving new inventions of affordable electric transportation, smart devices and wearable tech apparel which are in heavy demand by consumers who will gladly pre-order on crowdfunding sites. see Three Trends That Will Drive Crowdfunding in 2017, Entrepreneur Magazine online (1/2017).

Second, in 2016, the Securities and Exchange Commission finally adopted regulations initially authorized by the JOBS Act of 2012 that would allow crowdfunding sites to raise equity for startups by selling stock and securities directly to the public (subject to additional restrictions) without being subject to the onerous provisions governing traditional securities offerings. See SEC Guide. More recently, ICOs - initial coin offerings - which involves raising funds via cryptocurrency-based crowdfunding have gained popularity and further drive the growth of crowdfunding. See also ICOs as New Chapter for Crowdfunding, Lexology (12/12/2017); Indigogo To Host ICOs, Finance Magnates (12/13/2017)(reporting on campaign that plans to raise $5 million through ICO to form league of American football teams that use crowdsourced wisdom to choose players).

With the rise of divisive political policies, crowdfunding has seen an additional surge in growth. gained visibility in recent years. See e.g. D. Lithwick, They Have Lawsuits, You Have Money, Slate (10/2017)(describing use of crowdfunding platforms to challenge Trump Immigration policies); Neo Nazi Sympathizers Crowdfunding, CNET (12/4/2017)(reporting on rise of white supremacist-specific crowdfunding sites, following ban of these groups from other mainstream crowdfunding sites).
**KEY LEGAL ISSUES:**

**Compliance issues:** Crowdfunding sites that sell security must register with the SEC and adhere to regulations on disclosures and advertising or face investigation and potentially class actions by disgruntled investors. See *Tezos, a Company That Raised $232 Million In Crisis*, Ars Technica (11/17/2017) (reporting on lawsuit and potential SEC investigation against blockchain company that crowd-raised $232 million in equity but characterized investor purchases as “donations” to evade SEC registration requirements). Some states have adopted regulations for crowdfunding sites which must also be followed.

**Fraud/Consumer Protection:** Companies that crowdfund products with advance purchases but fail to deliver, or that ultimately deliver sub-standard products without the promised features may be subject to enforcement actions by the FTC or state AG’s offices (See e.g., *Radiate Athletics Kickstarter Program Sued*, BizJournals.com (11/5/2015) and *Crowdfunded Company Pays for Shady Deal*, US AG Press Release (2016) (describing successful enforcement actions by Pennsylvania and Washington State AG Offices to recover refunds from companies that fail to deliver promised crowdfunded products) and class actions. See also *Black et. al. v. Shezen Sunshine, 2-17-cv-02370 (N.D. Calif. 2017)* (class action against drone company that misrepresented features of drone on crowdfunding site). Fraud is also a growing concern about fake ICOs (See [https://btcmanager.com/summary-ico-conference-berkeley/](https://btcmanager.com/summary-ico-conference-berkeley/)) although there is as yet, little guidance from the SEC as to its plans for regulating ICOs.

**IP Issues:** Because crowdfunding campaigns often involve new inventions, they implicate several IP considerations such as whether a product requires IP protection, or conversely, infringes on IP rights of an existing company. Moreover, the public nature of crowdfunding sites makes it easy for overseas companies to knock off products in violation of IP laws. See *Getting Your Invention Off the Ground With Crowdfunding*, IPWatchdog (6/29/2013) (describing infringement actions against companies offering popular Kickstarter products and IP theft).
Future Trends & Opportunities:
So long as crowdfunding remains a potential source of revenue for startups, opportunities abound for lawyers to advise startups on compliance, or to represent disgruntled customers in class-actions. Meanwhile, the law will continue to evolve for newer crowdfunding initiatives, such as securities sales and ICOs.

Crossover Practice Areas:
Startup Law, IP, Finance, Securities Regulation.
BONUS: Can You Ethically Crowdfund a Law Firm or Litigation?

Lawyers are also availing themselves of crowdfunding platforms - either to raise money to start a law firm (e.g. Kellie Furr campaign on Indigogo) or to fund litigation through platforms like Crowdjustice - a crowdfunding platform exclusively to support public interest or civil rights suits worldwide - or GoFundMe, typically used to fundraise for personal causes. Not surprisingly, crowdfunding raises legal ethics questions that lawyers should keep in mind before launching a campaign:

Crowdfunding to Start a Law Firm - NYSBA Ethics Opinion 1062 (2015) responded to an inquiry from two recent law graduates seeking guidance on the ethics of crowdfunding to raise money to start an immigration law firm. The attorneys proposed to reward donors for their contribution by providing them whitepapers and informational briefings, or providing pro bono work for third party organizations of the donor’s choice. The Opinion held that the proposed crowdfunding was permissible so long as the firm did not give contributors an investment or interest in the firm. The Opinion also blessed the proposed “rewards” with the caveat that any informational material could not offer “legal advice” and any pro bono services complies with applicable ethics duties regarding conflict of interest and competency.

Crowdfunding Litigation: In Opinion 2015-6, the Philadelphia Bar Association’s Professional Guidance Committee (“Committee”) concluded - with numerous caveats - that ethics rules do not, as a general matter, forbid the use of crowdfunding to collect donations that will serve as a lawyer’s fee. For example, the Committee considered that crowdfunding raised the possibility of an unreasonable fee if all the money collected was paid to the lawyers, irrespective of the amount of work performed on the case. Thus, the Committee cautioned that to comply with fee rules, lawyers must place money in trust to draw down as the fee is earned, and to refund any excess amounts. Other requirements for use of crowdfunding include: (1) obtaining client consent to use crowdfunding to cover fees (Rule 1.8 - governing 3rd party payments); (2) abide by the duty of confidentiality in describing the case while at the same time, not mislead potential donors about the nature of the case (Rule 4.1 on misleading statements) and (3) hold funds collected in trust.
CRYPTOCURRENCIES

WHAT IS IT?

Cryptocurrency is exactly what its name implies – digital money. Bitcoin was the first - and perhaps best known cryptocurrency, but there are many others. Cryptocurrency law encompasses those issues that arise out of creation and regulation of, or investment in cryptocurrencies and use of cryptocurrency to purchase and sell goods or services. Complicating the legal issues further is the fact that cryptocurrency is global and subject to a patchworking of often conflicting laws of different countries.

In very, very simplistic terms, cryptocurrency works like this: a person purchases/creates an electronic “wallet” that has its own encryption key code; transactions are peer-to-peer (i.e., without an intermediary); transactions are verified by network nodes (i.e., the computers or servers which measure the active wallets on the network) and anonymously recorded in a publicly maintained ledger called a blockchain; and, the value of the cryptocurrency is determined by public use and perception via the marketplace (in other words, it has value because people think it has value).

The use of cryptocurrency removes the centralized bank – you transfer bitcoins (really, percentages thereof), stamping the transaction with your unique encryption key code; the transfer is recorded in the blockchain (e.g., “A gives X bitcoins to B”); the transaction is verified by “miners” before it becomes a permanent entry; and, once confirmed, a transaction can never be reversed. Miners are people who operate computer farms in a race to solve highly complex algorithms to find the “hash” (i.e., a product of the cryptographic function) that connects the new block with its predecessor; this connection verifies the transaction and forms a new block that is added to the chain of transactions.

WHY NOW?

It’s the modern-day gold rush (with its investment value having a similar volatility). In fact, in the first half of 2017, 1 bitcoin surpassed the spot price of an ounce of gold for the first time and on May 1, 2017 was valued at $1,402.03. Subsequently, the bitcoin was split into two derivative digital currencies: the classic bitcoin (BTC) and the Bitcoin Cash (BCH). As of February 2015, over 100,000 merchants and vendors accept bitcoin as a payment, with the number of businesses accepting bitcoin increasing exponentially. A 2017 Cambridge University study reports that there are 2.9 to 5.8 million unique owners of cryptocurrency wallets.

KEY LEGAL ISSUES:

Cryptocurrency is, for all intents and purposes, new; most people don’t understand it and others don’t know about it or don’t trust it. There are so many legal issues that have yet to arise, but here are some issues that have already popped up:
Constitutional issues: Specifically, the authority to “coin money” and “regulate the value” is convoluted by digital currency. Currently, Congressional action is in the exploratory phase, with the Government Accountability Office just being asked by the Senate Finance Committee to review tax requirements and compliance risks.

Under the Bank Secrecy Act (BSA), 143 banks and other financial institutions are subject to various registration and recordkeeping requirements. All “money service businesses” are required to register with the Department of the Treasury and develop anti-money-laundering and customer identification programs. In March 2013, FinCEN extended these rules to cover certain participants who transact in “convertible virtual currencies.” Exchangers and administrators are potentially subject to regulation if they function as money transmitters. By contrast, end users of bitcoin are expressly exempt as are miners who mine bitcoin for personal use. Miners who sell bitcoin could be considered a transmitter and potentially subject to regulation. See 2013 FinCEN Guidance. In 2015, FinCEN brought the first enforcement action against a virtual currency company, Ripple, alleging that it sold virtual currency for several months without a proper anti-money-laundering (AML) program in place, failed to designate a compliance officer, and did not solicit an independent review of its practices and procedures. See U.S. DEPT OF JUSTICE, SETTLEMENT AGREEMENT WITH RIPPLE LABS, INC., at app. A 4–6 (May 5, 2015).

Federal Tax Laws: The IRS has not done anything to address the tax implications of virtual currency, instead issuing guidelines that it will be treated as property for tax purposes and a taxpayer must apply tax law accordingly. See http://www.irs.gov/uac/Newsroom/IRSVirtual-Currency-Guidance. Yet, with the total anonymity of cryptocurrency transactions, how does the IRS verify proper reporting? The big case pending is: United States v. Coinbase Inc., Case No. 17-cv-01431 (ND CA 2017), where the IRS is seeking to compel Coinbase to hand-over account holder information to some 50,000 Coinbase users, hoping to dox account holders (i.e., uncover names, addresses, and other related information) who may have unde-reported taxable income from Virtual Currency holdings in tax years 2013-2015.

Criminal Counterfeiting: Current monetary laws do not mention digital currency in the prohibition to counterfeit both U.S. and foreign currency; it is unclear if there is a role or responsibility for the U.S. legal system to intervene if counterfeiting of cryptocurrency should arise (while it is claimed to be impossible, never say never).

Stamps Payment Act - This statute criminalizes the issuance, circulation, or pay out of “any note, check, memorandum, token or other obligation, for a less sum than $1, intended to circulate as money or to be received or used in lieu of lawful money of the United States,” and could apply to cryptocurrency if it were to become a legitimate competitor of the U.S. Dollar.

Election Law - How can we ensure that the United States Elections will not be compromised, and the Federal Election Campaign Act, as well as the Supreme Court ban on foreign campaign donations, be enforced if anonymous cryptocurrency exchanges are used during campaign? How will this affect the reporting of SuperPACs of its donors?
Fraud/Theft - The cryptocurrency system, like all internet based technology, is vulnerable to large security breaches and cyber-attacks; loss of encryption keys are hard to prove. In 2014, Mt. Gox declared bankruptcy after bitcoins worth $460 million were apparently stolen. Most recently, Bitstamp (a large European exchange), lost 19,000 bitcoins/$5 million in digital security breach. Consumers are also targeted for blockchain scams by enticing you to purchase non-existent products. On September 19, 2017, Reuters reported that Switzerland’s financial watchdog, FINMA, shut down Quid Pro Quo Association, a provider of fake cryptocurrency, and FINMA was investigating a dozen possible fraud cases. Some experts have expressed concern that bitcoin is a major Ponzi scheme yet to be uncovered.

Securities Regulation: Although bitcoin is not a definitely a security subject to direct regulation by the SEC, the agency, in a July 2017 statement, has stated that in some instances, sales of tokens by a virtual agency such as the DAO may be considered securities subject to SEC regulation. The SEC has issued several investor alerts regarding cryptocurrencies and red flags for investors. Meanwhile, the Commodities Futures Trading Commission defines bitcoin as a commodity. See also Blockchain Section (can companies add Blockchain to their name?)

Illicit Activity - The online drugs marketplace, Silk Road, was just recently shut down, but there are (and undoubtedly will be) more black market merchants of illicit and illegal drugs – users, delivery means and other aspects of nefarious activity is difficult to track with the use of cryptocurrency. A recent criminal case involved a seizure of $18 million in bitcoin transactions which were traced to Silk Road servers in Iceland. See US v. Ulbricht, 858 F.3d 71 (2nd Cir. 2017). Similarly, hackers use ransomware to target all kinds of companies, holding their servers and networks hostage (thereby shutting down the company) unless a ransom is paid via cryptocurrency – how can you stop that thief in the night?

Banking Regulations - There has been no guidance or regulations issued for banks to deal with cryptocurrency. Federal Reserve chair, Janet Yellen, said in the 2014 February statement: “Bitcoin is a payment innovation that’s taking place outside the banking industry… There’s no intersection at all, in any way, between Bitcoin and banks that the Federal Reserve has the ability to supervise and regulate.” There has been small steps on a state level, such as New York’s Department of Financial Services, to devise necessary regulation.

International Issues: Although bitcoin is lawful in the United States, to complicate matters, each sovereign country can accept or reject the legitimacy of cryptocurrency - and to date, countries’ approaches are, quite literally, all over the map. Ecuador, Bangladesh, Iceland, Russia Kyrgyzstan, and Thailand outright banned the currency. Starting in September 2017, all currency exchanges were being shut down in China. As of September 2017, both Japan and Norway accepted bitcoin, while Russia and India announced their intent to legalize cryptocurrency exchanges, but have not acted.
**Future Trends & Opportunities:** David Silver, founding partner in the Silver Law Group in Coral Springs, Florida and representative of several clients in cryptocurrency fraud cases, said: "There’s no sense in saying that cryptocurrencies are the wave of the future—they’re already here[.] ... Understanding the legal implications of the blockchain is another attorney growth area for a profession that desperately needs growth areas. Teaching tomorrow’s lawyers how to operate in a new world order is something every law school should be doing[.]"

**SIDE BAR - Law Firms and the Ethics of Cryptocurrencies:** As the use of digital currency becomes widespread, clients will come to expect law firms to accept it as a form of payment, just like making ACH or credit card payments online. And, lawyers know, that the more types of payments you accept, the more you are marketable and appealing to potential and current clients. But what are the ethical ramifications of accepting cryptocurrencies for legal services? but For

As far back as 2014, big name law firms began accepting payments (or partial payments) for services rendered via cryptocurrency. Like all payment for legal services, the charge should be reasonable related to the work involved. However, the fluctuation in price of cryptocurrencies leaves lawyers in a legal conundrum. On one hand, a price drop could leave the lawyer working for almost nothing. On the other hand, a price increase could effectively cause a lawyer’s rate to be “unconscionable.” Accepting cryptocurrency as a retainer poses the unique problem of how the lawyer can manage a trust account given ever-fluctuating value of the currency. The simplest and seemingly best way to approach payment by digital currency is to address bitcoin payment in the client’s engagement letter; convert such to its cash equivalent in USD and place those funds into a trust account in a bank with the client’s knowledge; and, note the number of bitcoins and the market value at conversion as part of the reconciliation and billing process.

Nebraska adopted this approach in Ethics Advisory Opinion 17-03 (September 2017), the first state opinion on the legal ethics of accepting cryptocurrency as payment. The Opinion concluded that an attorney may receive and accept digital currencies such as bitcoin as payment for legal services so long as the attorney immediately converts the digital currency into U.S. dollars to guard against possible overpayment resulting from bitcoin’s wildly fluctuating values. Ethics Ronald Rotunda criticized the Nebraska opinion, arguing that the matter of fluctuating currency value isn’t an ethics issue, but one of potential financial risk. After all, attorneys are may ethically receive stock shares as payment and are not required to immediately cash them upon receipt. For additional discussion of ethics issue see also Controversies Over Acceptance of Bitcoin, OC Bar (2014) and Nelson & Siemek, What Lawyers Need to Know About Accepting Bitcoin, Wisc. Lawyer (Jan. 2015).
Cyberbullying is truculent behavior which occurs over electronic communication through apps or social media sites (SMS), text messaging, instant messaging (IM), email, web forums, or gaming, where people can view, participate or share content; it is usually done anonymously. Cyberbullying is sending, posting or sharing negative, harmful, false or mean content about another person to cause embarrassment or humiliation. The behavior may take several forms:

**Cyberharassment:** repeatedly sending offensive or malicious messages to torment victim; usually used synonymously with cyberstalking, but does not include credible threat of harm, rather is embarrassing or humiliating victim

**Cyberstalking:** pattern of repeated and unwanted harassment, contact, threatening or malicious behavior via the internet, email, or other electronic communications involving a credible threat to harm directed at a specific person that would cause a reasonable person to feel fear

**Denigration:** posting online messages through email, instant messaging, chat rooms, or websites set up to ridicule, gossip or spread rumors about the victim

**Digital self-harm:** occurs when a person anonymously sends himself/herself instructions for self-harm or self-injury

**Dissing:** sending or posting cruel information (including photos, screenshots or videos) to damage a person’s reputation or friendships with others; usually done by someone the victim knows

**Doxing/Doxxing:** publishing or making available personally-identifying information about a person; exposes victim to an anonymous mob of countless harassers, calling their phones, sending them email, and even appearing at the victim’s home (#GamerGate)

**Exclusion:** intentionally leaving victim out of online groups (e.g., IMs, SMS, forums, etc.) and malicious or harassing comments are made about the victim

**Flaming:** online fights or bullying (usually through emails, IM or forums) that directs hard, rude, angry and/or vulgar languages or images to a specific person
Fake Profiles/Masquerading: fake identity is created by a person who typically knows victim quite well and used to harass the victim anonymously (note: catfishing is a romantic extension, discussed infra)

Frapping: (combination of “Facebook” and “Rape”) when someone logs into another’s SMS, email or phone (usually victim has accidentally stayed logged in) to impersonate the victim and post inappropriate content in their name (#AndersonCooper)

Happy-Slapping: a physical attack of the victim by a group of people which is photographed or video recorded (commonly with a camera or smartphone), and posted or published online to embarrass the victim

Impersonation/Imping: pretending to be the victim online and post inappropriate content in their name

Subtweeting or Vaguebooking: subtle posts that never mention victim’s name, yet audience knows who the posts are referencing; to avoid detection by teachers, administrators or parents

Trickery: the victim is persuaded to reveal personal information that they would not otherwise reveal, which is then publicly shared

Trolling: deliberate act of provoking a response through the use of insults or bad language on online forums and social networking sites

Outing: posting or publicly sharing private information, pictures or videos of the victim

WHY NOW?

Practically everyone in the world uses the internet (see the profiles on Social Media, and First Amendment and Online Defamation); according the U.S. Supreme Court, in Packingham v. North Carolina 137 S. Ct. 1730 (June 19, 2017), social media is the “modern public square.” There are, however, negative consequences to the growing use of the internet and social media. Just recently, on November 9, 2017, Sean Parker, co-founder of Napster and first president of Facebook, stated during an Axios interview with Mike Allen, that Facebook creators knew they were creating something addictive that exploited “a vulnerability in human psychology” from the outset, and further lamenting, “God only knows what it's doing to our children's brains.” On November 10, 2017, at the Stanford Graduate School of Business, View from the Top event, Chamath Palihapitiya, former Facebook Vice President of User Growth (2007-2011), said that the use of social media is a danger for society, stating that the it is “ripping apart the social fabric of how society works” and he feels “tremendous guilt” for helping build Facebook into the behemoth it is today; he will not let his children use it. (Note: On December 12, 2017, Facebook spokesperson responded that Mr. Palihapitiya was not part of the company for over six (6) years and the company is constantly changing with “a lot of work and research with outside experts and academics to understand the effects of our service on well-being, and we’re using it to inform our product development.”).

One of those dangers is cyberbullying, which is considered a global epidemic taken root in affecting society at all levels (i.e., victims may be children, teens or adults). Cyberbullying is considered more
severe than “traditional” bullying because it is 24-7 with a widespread audience (and participants), with tragic consequences. Due to the anonymity of the actions, it can be nearly impossible to trace the source, and, once posted, it is extremely difficult to remove/delete the offending material.

While every aspect of society can be victimized by cyberbullying, children are considered the most vulnerable. According to the U.S. Department of Health & Human Services (HHS), kids who are the victims of cyberbullying are more likely to use drugs and alcohol, skip school, get bad grades, and have low self-esteem, also known to have increased instances of health problems, depression, and anxiety that in rare cases have led to violent retaliation or suicide.

KEY LEGAL ISSUES

**Federal Law:** Currently, there is no federal law or policy against cyberbullying. In 2008, the Megan Meier Cyberbullying Prevention Act (H.R. 1966) was introduced to Congress, but was not enacted largely due to contradictions with the First Amendment and freedom of speech (see, e.g., the First Amendment and Online Defamation profile). See U.S. v. Drew, No. CR 08-0582-GW (C.D. Ca.), where defendant (an adult) created a fake SMS profile to spy on, befriend and flirt with victim (child) in her daughter’s class (i.e., catfishing, discussed infra), and subsequently told victim he no longer liked her and “the world would be a better place without her in it,” causing victim to commit suicide. The court granted defendant’s motion for acquittal pursuant to Fed. R. Crim. P. 29(c), vacating the grand jury convictions of three violations under the Computer Fraud and Abuse Act based upon defendant’s breach of the MySpace Terms of Service. See id., 259 F.R.D. 449 (C.D. Ca. August 28, 2009) (treating a violation of the website’s terms of use agreement, without more, as a statutory violation ran afoul of the void-for-vagueness doctrine and it was unclear whether every intentional breach of a website's terms of service was equivalent to an intent to access the site without authorization). In 2013, the Tyler Clementi Higher Education Anti-Harassment Act was introduced to require colleges and universities to have anti-harassment policies and expanded bullying prevention programs; the proposed Act was reintroduced to Congress on April 27, 2017 and currently pending. See State v. Ravi, Docket Nos.: A-4667-11T1, A-4787-11T1. Tyler Clementi committed suicide after his Rutgers University roommate used a webcam to observe and publish victim’s homosexual activity; defendant was convicted of multiple counts of invasion of privacy, bias intimidation, and other crimes, but all convictions were overturned because the main predating statute N.J.S.A. § 2C:16-1(a)(3) was deemed unconstitutional (see id., 447 N.J. Super. 261 (Sup. Ct. Sept. 9, 2016)); defendant accepted plea deal on October 27, 2016 to one count of attempted invasion of privacy and sentenced to time served (20 days in jail, with credit of 5 days good behavior and 5 days work release) and fines paid.

There are some federal civil and criminal protections against harassment in public, federally-funded schools which also includes discipline for off-campus behavior that results in a substantial disruption of the learning environment in school (see, e.g., Campus Defense profile). There are also several federal statutes which have
been applied to individuals when cyberbullying/cyberstalking crosses into criminal behavior (note: terms “interstate or foreign commerce” include phone, computer, internet, etc.):

17 U.S.C. § 50 Copyright Infringement: Victims of nonconsensual online publication of intimate photographs or videos (i.e., revenge porn) may bring a civil suit for copyright infringement if the victim is the person who originally took the picture, and is thus the copyright owner.

18 U.S.C. § 875 Interstate Communications: federal crime to transmit any communication in interstate or foreign commerce containing a threat to injure another person, or publishes or threatens to publish private photos or video of another with intention of forcing victim to do something they may not otherwise have done (i.e., extortion). See, U.S. v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997) (the “Jake Baker” case), statute is construed to apply only to communications of actual threats, not where a cyberstalker engaged in a pattern of conduct intended to harass or annoy another (absent some threat); and Elonis v. U.S., 135 S. Ct. 2001 (2015) (government must also prove the defendant knew or was recklessly indifferent to the threatening nature of the communication). See also, e.g., U.S. v. Howard, 759 F.3d 886 (8th Cir. 2014) (defendant convicted of extorting victim through threats of outing his sexual orientation to employer, and sending nude photos of victim to other employees and colleagues); and U.S. v. Petrovic, 701 F.3d 849 (8th Cir. 2012) (defendant convicted when threatened to send and subsequently sent photos and videos of victim when nude or engaging in sexual activity with derogatory language to victim’s friends, family, co-workers, and launched a website with same images and personal information (e.g., her children’s social security numbers) and demanded money to remove website).

18 U.S.C. § 1030 Computer Fraud and Abuse Act: civil and criminal liability for a person who obtains any information from any internet-connected computer without authorization and/or access to defraud (note: computer hacking to obtain explicit photographs or other information belonging to the victim). See, e.g., Drew, supra; U.S. v. Wadford, 331 F. App’x 198 (4th Cir. 2009) (where defendant gave coworker-victim a date rape drug while they were on an interstate business trip and took photographs of her naked from the waist down while she was unconscious; after defendant terminated, he hacked co-worker’s email accounts to send false, fraudulent, and threatening emails to other coworkers, including attachments of aforementioned photographs); and U.S. v. Ledgard, 583 F. App’x 654 (9th Cir. 2014) (defendant hacked into ex-girlfriend’s online account to overdraw her bank account, max out her credit card, and send graphic sex photos of the victim to her family, friends, and coworkers).
18 U.S.C. § 1952 Travel Act: prohibits the use of a facility in interstate or foreign commerce to engage in extortion. Although "extortion" is not defined under the Travel Act, courts uphold its application in cases where defendant attempts to extort money by threatening to expose victim’s sexual activities (note: currently is sextortion). See, e.g., U.S. v. Nardello, 393 U.S. 286, 295-96 (1969); and U.S. v. Hughes, 411 F.3d 461 (2d Cir. 1969).

18 U.S.C. § 2251 Production of child pornography: prohibits using, employing, persuading, and coercing a minor to produce child pornography, or attempting to do so; applicable where the defendant enticed or coerced a minor victim into taking and sending sexually explicit images or videos, or engaging in sexually explicit conduct over a webcam.

18 U.S.C. § 2261A(1) Interstate Stalking Act: federal crime for any person to travel across state lines with the intent to injure or harass another person and, in the course thereof, places that person or a member of that person’s family in a reasonable fear of death or serious bodily injury (note: requires stalker physically travel across state lines makes it largely inapplicable to cyberstalking cases).

18 U.S.C. § 2261A(2) (note: enacted and amended as part of the Violence Against Women Act and subsequent reauthorizations): federal crime to use the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to intentionally harass and cause someone substantial emotional distress; requires a course of conduct with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person (note: amendment in 2013 eliminated the requirement that the victim and the perpetrator be in separate jurisdictions) See, e.g., U.S. v. Matusiewicz, Criminal Action No. 13-CR-00083 (D. Del.), where three defendants were sentenced to life in prison for the murder of defendant’s ex-wife and her friend after engaging in a three-year to stalk, harass, and intimidate the ex-wife and her children; U.S. v. Sayers, 748 F.3d 425 (1st Cir. 2014); U.S. v. Osinger, 753 F.3d 939 (9th Cir. 2014) (affirmed judgment for § 2261A(2) violations and no First Amendment protection for defendant who created false Facebook account in victim’s name with sexually explicit photographs and sent sexually explicit photographs of victim to victim’s co-workers and friends)).
18 U.S.C. § 2422(b) Enticement/coercion of a minor: prohibits the use of a facility of interstate commerce (i.e., internet) to persuade, coerce, or entice a minor to engage in sexual activity or to attempt to do so (note: commonly used in sextortion cases involving minors).

18 U.S.C. § 2425 Transmit Information About a Minor: prohibits use of any means of interstate or foreign commerce to knowingly communicate with any person with intent to solicit or entice a child into unlawful sexual activity (note: it does not reach harassing phone calls to minors absent a showing of intent to entice or solicit the child for illicit sexual purposes).

18 U.S.C. § 2511 Eavesdropping: civil and criminal liability for non-consensually published material that was originally obtained by interception of an electronic communication.

47 U.S.C. § 223 Telecommunications: prohibits the use of a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the called number; perpetrator need not reveal his/her name (§§(a)(1)(c)), but communication (not conversation) must be directly between perpetrator and victim (note: covers calls and texts, not cover use of internet, such as email, SMS or websites). See U.S. v. Popa, 187 F.3d 672 (D.C. Cir. 1999) (statute does not apply to conversations that lack intent to threaten, and First Amendment protects speech intended to engage in public or political discourse).

State Laws: All fifty (50) states and D.C. have bullying laws, with various criminal punishments depending upon the act (e.g., assault for physical hurting of another). However, only forty-eight (48) states and D.C. include electronic harassment, with eighteen (18) including criminal sanctions and twelve (12) having proposed criminal sanctions. In every state except Montana, the bullying laws mandate schools to have a formal policy for identification of behavior and discipline.

School Discipline: Guidelines and penalties vary from state to state, and those with school policies leave punishment determinations up to the school; though states like California, however, clearly states the school can suspend or permanently expel offenders based on each individual case (i.e. “Seth’s Law”). See, e.g., Dunkley v. Bd. Of Educ. Of the Greater Egg Harbor, Case No. 14-7232, 216 F.Supp.3d 485 (D. N.J. Oct. 20, 2016) (court granted defendant's motion for summary judgment and denied plaintiff's cross-motion for summary judgment, upholding the school district’s nine (9) day suspension and formal juvenile complaint with the Atlantic County Prosecutor's Office for the posting of out-of-school YouTube video and Twitter postings (50-100 followers) regarding other students that the school determined to be in violation of the state's anti-bullying statute and the school's anti-bullying policies).
“[U]nder the law governing speech by students in and out of school, in conjunction with the purpose and goals of the Anti-Bullying Act, the Court finds that plaintiff’s First Amendment rights, and the attendant procedural rights under N.J.A.C. 6A:16-7.6 and the Anti-Bullying Act, were not violated by his vice-principal, the school resource officer, or the school board.” Id. at 496. See also Kowalski v. Berkeley Co. Sch., 652 F.3d 565 (4th Cir. July 27, 2011) (upheld summary judgment in favor of defendant for five (5) day school suspension and ninety (90) days social suspension after student used her home computer to create a webpage that was largely dedicated to ridiculing a classmate). But see Layshock v. Hermitage Sch. Dist., 650 F.3d 205 (3d Cir. June 13, 2011) (upheld summary judgment in favor of student that used grandmother’s computer to create a parody profile of his Principal with derogatory postings; “student expression may not be suppressed unless school officials reasonably conclude that it will materially and substantially disrupt the work and discipline of the school.”); J.S. v. Blue Mountain Sch. Dist., 650 F.3d 915 (3rd Cir. 2011) (student online profile of principal not disruptive, protected by First Amendment); J.C. ex rel. R.C. v. Beverly Hills Unified Sch. Dist., 711 F. Supp. 2d 1094 (C.D. Cal. 2010) (off-campus video of fellow student not disruptive, author can’t be suspended); Rosario v. Clark Cnty. Sch. Dist., Case No. 2:13-CV-362 JCM, 2013 U.S. Dist. LEXIS 99363 (D. Nev. July 3, 2013) (permitted student’s First Amendment challenge to discipline for student’s derogatory tweets against coach and team).

**Criminal Prosecutions** - Many states have their own criminal prosecutions of minors and adults that commit cyberbullying related crimes. See, e.g., People v. Kucharski, 987 N.E.2d 906 (Ill. App. Ct., Mar. 29, 2013), app. den’d, 2013 Ill. LEXIS 1225 (Ill., Sept. 25, 2013) (upheld conviction of harassment through electronic communications from defendant’s actions in accessing his former girlfriend’s MySpace page and posting comments and a photograph of her); In re Rolando S., 197 Cal. App. 4th 936 (Cal. App. 5th Dist., July 21 2011), review den’d, 2011 Cal. LEXIS 10793 (Cal., Oct. 19, 2011) (juvenile defendant prosecuted for receiving an unsolicited text message with the victim’s email password and using the password to gain access to the victim’s Facebook account, as well as altering the account and posting several sexually inappropriate messages from the victim’s account); State v. Canal, 773 N.W.2d 528 (Iowa Sup., Sept. 18, 2009) (affirmed jury conviction of defendant for knowingly disseminating obscene material to a minor, where 18 year old sexted fourteen-year-old female classmate). But see, People v. Marquan M., 994 N.Y.S.2d 554 (2014) (lower court erred in denying defendant’s motion to dismiss cyberbullying charges in criminal case because New York cyberbullying law was overbroad).

A recent case that received widespread media attention as a groundbreaking conviction in a texting-suicide case, which charges were for involuntary manslaughter rather than cyber bullying type laws. In Cmwlth. v. Carter, No. 15YO0001NE (Mass. Juv. Ct. June
Michelle Carter was found guilty of involuntary manslaughter when she encouraged her then-boyfriend, Conrad Roy III, to commit suicide by communicating with him over intimate text messages and one crucial phone call; she was subsequently sentenced to 2.5 years, which is stayed pending her appeals. The decision came after the Massachusetts Supreme Judicial Court denied a motion to dismiss for lack of probable cause in this case, saying that words could be a sufficient basis for finding causation based on the logic that a person could be “virtually present.” See id., 474 Mass. 624 (July 1, 2016).

**Civil Liability** The filing of civil liability lawsuits, particularly against school districts for failure to protect students, are increasing; with claims of Title XI violations, equal protection, emotional distress, libel, negligence, etc. See, e.g., Mihnovich et al v. Williamson Co. Bd. of Educ. et al, Case No. 3:2013cv00379, 2014 U.S. Dist. LEXIS 155169 (M.D. Tenn. Nov. 3, 2014) (defendant’s motion for summary judgment denied because questions of fact about nexus between racially offensive texts and Facebook posts and victim’s school experience bar summary judgment on Title VI cyberbullying claim). See also Logan v. Sycamore Cmty. Sch. Bd. of Educ., Case No. 1:09-cv-885-SAS (S.D. Oh. filed Dec. 2, 2009) where victim committed suicide after ex-boyfriend published nude photos she gave to him (i.e., “sexting”), resulting in cyberbullying on Facebook, MySpace and texts; victim’s parents sued the school district under 20 U.S.C. § 1681 (freedom from sex-based discrimination), 42 U.S.C. § 1983 (equal protection), intentional infliction of emotional distress, and invasion of privacy tort. The lower court denied defendant’s motion for summary judgment on plaintiffs’ Title IX and 42 U.S.C.S. § 1983 claims and granted defendant’s motion for summary judgment on plaintiffs’ negligent infliction of emotional distress claim (see id., 2012 U.S. Dist. LEXIS 77474 (S.D. Oh. June 5, 2012)); and the case subsequently settled on October 9, 2012 (with monetary compensation and attorney’s fees). The State of Ohio also enacted the Jessica Logan Act (effective Nov. 4, 2012), with one of the main provisions of the Act is to required schools to prohibit cyberbullying and expand anti-harassment policies. Compare Witsell v. Sch. Bd., Case No. 8:11-cv-781-T-23AEP, 2012 U.S. Dist. LEXIS 28603 (M.D. Fla., Mar. 5, 2012) (where victim committed suicide after regular cyberbullying following publication of her sexting and meeting with school social worker; case against school for allegedly failing to take appropriate action after learning the teen had suicidal thoughts dismissed because “a school board typically owes no constitutional duty to protect a student from self-inflicted harm that occurs outside of school).

Cases against the harassing peers and their parents are on the rise. See Boston v. Athearn, Case No. A14A0971, 329 Ga. App. 890 (Ga. Ct. App. Oct. 10, 2014), landmark decision in libel action involving a teen creating a disparaging fake Facebook account in plaintiff’s name attributing to plaintiff racist and other offensive views and stating plaintiff had mental health disorders, used illegal drugs, and was homosexual, the Georgia’s highest court reversed summary judgment ruling in defendant’s favor, holding that a reasonable jury could find that they proximately caused some part of the victim’s injuries by allowing the false and offensive statements remaining on display and continue to reach readers, for an additional
11 months after learning of their teen’s actions; the parents of the 7th grader that created the page were potentially liable for negligence for not forcing him to close the account once they learned of it. See also Sheila Pott, et al. v. John B, Case No. 113CV244689 (San Jose, Ca), where victim’s parents sued three (3) boys and their parents, and others involved, for wrongful death in suicide of victim following the recording and dissemination of those recordings of her sexual assault during a high school party. The case settled prior to trial, with the homeowner paying $100,000.00; the girl who “covered it up” paying $150,000.00; one parent paying $25,000.00; and remaining two (2) boys agreed to verbally apologizing in open court, admitting the sexual assault and role in victim’s death, paying a combined $950,000.00, and other equitable relief. In addition, in an ancillary criminal case by Santa Clara District Attorney, all three teens were convicted of sexual assault charges in juvenile court after pleading guilty and two of them sentenced to 30 days in juvenile jail, which they served on weekends, and a third to 45 consecutive days.

Sexting/Sextortion Sexting (combination of sex and texting) is sending, receiving, or forwarding sexually explicit messages, photographs or images, primarily between mobile phones, but also includes use of a computer or any digital device. One of the biggest sexting controversies is from disgraced public figure, Anthony Weiner (#Weinergate), who resigned from Congress in 2011 after sending a sexually suggestive picture of himself to a 21-year old woman on twitter; his failed New York City mayoral race after admitting to sexting three (3) more women since his prior resignation; and, perhaps, the most well-known incident is his guilty plea on May 19, 2017 to one count of transferring obscene materials to a minor for sexting a fifteen (15) year old girl (see U.S. v. Weiner, Case No. 1:17-cr-00307-DCL (S.D.N.Y.), for which he was sentenced to twenty-one (21) months in prison starting on November 6, 2017. See also, e.g., Miller v. Mitchell, 598 F.3d 139 (3rd Cir. 2010) (court granted plaintiff’s motion for preliminary injunction against district attorney who threatened to prosecute students for “sexting” in retaliation for student’s exercising constitutional right to not attend the sex-education program).

Sextortion is a form of sexual exploitation that employs non-physical forms of coercion to extort sexual favors from the victim, usually following sexting acts. In Harrison v. Clatskanie Sch. Dist. #6J, No. 3:13-cv-01847-ST (D. Or. filed Dec. 5, 2013), the plaintiffs filed a lawsuit against the school district, claiming they were victims of sextortion at the school when bullied into sending nude photos of themselves to boys at their middle school. The case ultimately settled on or about April 12, 2015, with the school paying $225,000.00 to the three (3) plaintiffs. Similarly, in State v. Stancl, Case No. 2009CF000134 (Wisc. filed 2009), defendant high school student impersonated girls on Facebook and formed online romantic relationship with at least thirty-one (31) boys in his school (catfishing); he enticed the boys (aged 15-18) to send him nude photos or videos (sexting); and, subsequently blackmailed at least seven (7) of the boys into having sex with him by claiming to release all photos and videos if they refused (sexploitation). In addition, Stancl took pictures of the sexual encounters. Stancl entered into a plea agreement, pleading no contest to
two charges—third-degree sexual assault and repeated
assault of the same child, and was convicted on both counts,
and sentenced to 15 years in prison (of a maximum possible
30) and 13 years of extended supervision.

**Catfishing** - This refers to the practice of setting up a fictitious
online profile, most often for the purpose of luring another into a
fraudulent romantic relationship. The Urban Dictionary defines a
"catfish" as: "someone who pretends to be someone they’re not
using Facebook or other social media to create false identities,
particularly to pursue deceptive online romances.” Currently,
Oklahoma is the only state with specific legislation on this cyber
issue, enacting the Catfishing Liability Act of 2016; hopefully it will
be a model in other states.

There are several notable catfishing cases. As previously mentioned
in the Megan Meier case (U.S. v. Drew, supra), her classmate’s
mother set up a fake MySpace profile to flirt with and spy on the
minor; ending the relationship with suicidal suggestions that
ultimately led the minor to taking her own life. Extensive media
attention was given to the 2012-13 catfishing hoax against Notre
Dame football star Manti Te’o by Ronaiah Tuiasosopo, who posed as
a girl online and in telephone messages in their exclusively online
relationship; Te’o fell in love with the fictitious girl and publicly
announced that he was told the girlfriend died of leukemia on
September 11, 2012 on the same day as his grandmother. In
Zimmerman v. Bd. of Trs. of Ball State Univ., 12-cv-01475-JMS-
DML, 940 F. Supp. 2d 875 (S.D. Ind. April 15, 2013), the court
upheld the university’s decision to suspend students for one (1) year,
with probation upon return and a no-contact order with the victim,
when the student engaged in an elaborate catfishing scheme
against his ex-roommate and then published a videotape of the
victim, claiming he was a pedophile. In People v. Faber, 15 Cal. App.
5th Supp. 41 (August 11, 2017), defendant was sentenced to six-
and-one-half (6.5) year jail sentence for 13 counts of violating
protective orders, when he engaged in a catfishing scheme (using
ten (10) different telephone numbers, and other electronic devices
to deceive victim) to contact and harass his ex-girlfriend.

Catfishing is also considered a huge romance scam where
perpetrators scheme money from the victim. The FBI reports that it
received 15,000 romance scam complaints in 2016 with losses
exceeding $230 million (estimating that only about 15% of those

In Picciano adv. OKCupid.com (N.Y. Sup. Ct. filed March 17, 2014), the plaintiff sued
OKCupid, its parent company IAC.com, and his banks for negligence
and false advertising, when he fell victim to a catfishing scheme on
the matchmaking website and lost $70,000.00 to the perpetrator;
plaintiff withdrew his complaint after OKCupid filed a motion to
dismiss.

**Bodyshaming** - The action or practice of humiliating someone by
making mocking or critical comments about their body shape or size.
In a pioneering prosecution against “body-shaming,” on May 24,
2017, Dani Mathers, a model and former Playboy Playmate, plead
no contest to a criminal charge of invasion of privacy after taking a
photo of a naked woman in an LA Fitness gym locker room and
posting it to Snapchat with the caption, “If I can’t unsee this then
you can’t either.” Ms. Mathers chose 30 days of community labor,
removing graffiti as her punishment. In October 2017, there has been a lot of media attention surrounding the shaming prank, #pullapig (a ‘game’ where guys try to hook up with the least attractive girls they can dupe on a night out), after Sophie Stevenson claimed she was the victim of this shaming hoax by Jesse Mateman. The alleged prankster has alternatively denied the allegations and threatened legal action for damages suffered because he is being publicly “threatened and demonized.” See Dani Mathers Plea Bargain for Body Shaming, TMZ (5/24/2017).

Revenge Porn/Nonconsensual Pornography - This is distribution of sexually graphic images of individuals without their consent via any medium. Slut-shaming (#slutshaming) has been used as a form of bullying on social media by criticizing persons for perceived violations of expected sexual behavior and appearances, with persons using revenge porn tactics against the victim. There are no federal laws against revenge porn; however, thirty-eight (38) states (AL, AZ, AK, CA, CO, CT, DE, FL, GA, HI, ID, IL, IA, KS, LA, MA, MD, MI, NH, NJ, NM, NC, ND, OK, OR, PA, SD, TN, TX, UT, VT, VA, WA, WV, and WI) and D.C. have revenge porn laws; only eleven (11) states (CA, CO, FL, MN, NC, ND, PA, TX, VT, WA, and WI) provide for civil remedies. In June 2017, the New York Senate passed a revenge porn bill, and the New York City Council voted in November 2017 to do the same, though neither has been signed into law. In New York’s first “revenge porn” case, People v. Barber, 2014 NY Slip Op 50193(U), 42 Misc.3d 1225(A) (Sup. Ct. February 18, 2014), the court granted defendant’s motion to dismiss all charges, including Aggravated Harassment in the Second Degree, when defendant posted nude photos of his ex-girlfriend on Twitter and sent copies to the victim’s employer and sister, without her consent; concluding that the conduct, while reprehensible, does not violate any of the criminal statutes under which he was charged. But see, Taylor v. Franko, Case No. 1:09-cv-00002-JMS-RLP (D. Hi. July 12, 2011) (before revenge porn statute, court granted plaintiff’s revenge porn claims based on invasion of privacy and emotional distress, and awarded $425,000.00); and Doe v. Hofstetter, Case No. 11-cv-02209-DME-MJW (D. Co. Aug. 14, 2012) (before revenge porn statute, court granted damages to plaintiff and her husband for revenge porn claims, as well as injunctive relief). In August 2014, Meryem Ali filed suit against Facebook for failure to timely remove a “revenge porn” profile page targeting her, and inviting her friends and family to visit the page (it was eventually removed); the parties must have reached a settlement, as the court granted a stipulation of dismissal on November 17, 2014 and terminated the case on November 18, 2014. See Ali v. Facebook, Inc., Case No. 4:14-cv-03066 (S.D. Tx. Nov. 18, 2014).

There have been many “first of its kind” rulings on this issue. In [Names Redacted for Privacy], No. 112CV233490 (Santa Clara Co. Super. Ct. Feb. 18, 2014), a jury in a California civil case returned a verdict of $250,000 to a victim of revenge porn, known as the first civil verdict for a porn revenge case in the country. The Texas Court of Appeals was the first to uphold damages awarded by a jury to a plaintiff in a revenge porn case, but reduced the amount to $345,000.00, finding that the jury and trial court wrongly awarded damages for intentional infliction of emotional distress and defamation. See Patel v. Hussain, Case No. 4-14-00459-CV, 485 S.W.3d 153 (Tx. Ct. App. Jan. 21, 2016) (ex-girlfriend claimed that
after the couple broke up, Patel hounded her with a slew of offensive and threatening communications, hacked or attempted to hack her accounts, and posted secretly recorded sexual videos of her on the Internet). See also People v. Iniguez, 247 Cal. App. 4th Supp. 1 (Cal. App. March 25, 2016) (court affirmed judgment of conviction following a jury trial of violation of California revenge porn laws when defendant posted nude photographs of his ex-girlfriend; said laws were not unconstitutional). In Hoewischer v. White (In re White), 551 B.R. 814 (Bankr. S.D. Oh. June 23, 2016), the Bankruptcy court granted summary judgment to plaintiff that her claims arising from debtor’s posting of judgment creditor’s nude photos on revenge porn website were nondischargeable as based on willful and malicious injury.

In the ongoing litigation, Mischa Barton adv. Jon Zacharias & Adam Spaw, filed in Los Angeles County, California, the actress obtained a permanent restraining order against her ex-boyfriend and his friend from coming within 100 feet of her and from disseminating x-rated videos of her that were taken without her knowledge or consent (that had been touted to online porn companies). Most recently, on November 22, 2017, an anonymous Twitter user posted explicit nude photos and texts of Republican Rep. Joe Barton without his consent, making him a victim of revenge porn; it appears to be a “clear cut” violation of laws criminalizing revenge porn and Capital Police are currently investigating. Rep. Barton maintained that the photos and messages were exchanged during a consensual relationship, but nevertheless announced his retirement in 2018 due to the scandal.

**Swatting** - This is a form of online harassment where emergency responders are deceived into dispatching Special Weapons and Tactics (SWAT) team to the location of the victim; either hackers break into the police system to make an alert or place a fabricated 911 call. While swatting might seem like a prank (and is widely seen in the gamer community), it is actually extremely dangerous, terrorizing the victim and placing both the victim and law enforcement at risk. There is no current federal anti-swatting law; though, prosecution can be done under existing federal statutes (as identified above, supra). See, e.g., U.S. v. Stuart Rosoff, et al., 3:07-CR-196-B (N.D. TX); and U.S. v. Weigman, Criminal No. 3:08-CR-171-M (N.D. TX. filed Jan. 26, 2009); see also Press Release, Dep’t of Justice, Individual Pleads Guilty in Swatting Conspiracy Case (Jan. 29, 2009) (the “Weigman Conviction” at (sentencing for involvement in a swatting conspiracy); Press Release, Dep’t of Justice, Last Defendant Sentenced in Swatting Conspiracy (Nov. 16, 2009) (the “Nalley Conviction” at and Press Release, U.S. Attorney’s Office, Man Faces Five Years in Federal Prison in ‘Swatting’ Case (July 29, 2014) (the “Neff Conviction” at

Rep. Katherine Clark unsuccessfully introduced the Interstate Swatting Hoax Act of 2015, following her own swatting experience. On June 27, 2017, Rep. Clark introduced the Online Safety Modernization Act of 2017 to address “cybercrimes against individuals,” including sextortion, swatting and doxing; it is currently pending before Congress. There are only a few states with anti-swatting laws, such as California (2014) (note: following a wave of swatting of a bunch of celebrities in 2013) and New Jersey (2015)
Future Trends & Opportunities: There is a significant national trend towards harsher legislation and criminal punishment towards all forms of cyberbullying, as well as more specific identification towards bullying trends in schools, states, and nationwide. Although all of the pending federal laws may be difficult to pass (due to First Amendment Concerns), the nationwide message is being sent loud and clear that cyberbullying will not be tolerated. As the rules and consequences continue to evolve, parents are and will always to be the frontline to protecting children and their online activity.

(note: the legislator sponsoring the bill was swatted after introducing it).
WHAT IS IT?

Broadly defined, cybersecurity law encompasses the laws and standards governing the safekeeping and protection of electronic data and the consequences that arise as a result of a breach of applicable laws and standard of care. Cybersecurity overlaps with privacy law to the extent that an attack on a system or unauthorized access to customer information violates privacy rights. However, the topic of privacy extends beyond breaches, and includes matters such as providers’ transparency in collection of data - and these issues are discussed under the topic of Privacy Information.

WHY NOW?

Today, more companies than ever are collecting and holding sensitive personal information - including retail merchants, health insurers and providers, credit bureaus and even law firms. Moreover, companies retain information in digital format which is stored either on local computer systems that are interconnected across servers or in the cloud, thus allowing more opportunity for interception. Even as companies plug these security gaps, hackers are gaining sophistication in penetrating security system, capitalizing on user error through phishing expeditions to unleash viruses.

KEY LEGAL ISSUES:

Unauthorized Access:  Is there civil or criminal liability for a given cyber-security intrusion or unauthorized access?  To answer this question, it is first necessary to determine what constitutes unauthorized access to a computer and is the conduct civil or criminal? Relevant statutes include Computer Fraud and Abuse Act, 18 U.S.C. §1030, identity theft statutes and applicable state laws.

Liability for Failure to Comply With Data Notification:  What is potential civil liability for an entity holding data that has been stolen - either for the intrusion itself or failure to comply with data breach notification? Relevant sources of law include breach notification statutes and state tort law for negligent security practices. A recent cautionary example is Uber’s November 2017 disclosure that hackers had stolen 57 million driver and rider accounts a year earlier, and that the company had paid the hackers $100,000 ransom and kept the breach a secret. See NYT (11/21/2017). Within two weeks of Uber’s untimely revelation, the City of Chicago and the Washington State AG have brought enforcement actions for
penalties for violation of disclosure laws and breach of privacy, seeking civil fines of up to $2000/violation, two class actions have been filed and a number of other states are also launching investigations. See Uber Data Breach Lessons, Govtech.com (12/2/2017).

**Regulatory Oversight:** Entities are potentially subject to an array of regulatory authorities related to cybersecurity standards - including Section 5 of the Federal Trade Commission statute (15 U.S.C. §45), HIPAA Statute, Gramm-Leach Bliley Act, SEC regulations/guidance and various state laws. As of October 2017, 48 states, as well as the District of Columbia, Puerto Rico and the US Virgin Islands all have enacted laws requiring notification of security breaches involving personal information. Alabama and South Dakota are the only states with no security breach law. See e.g., Chart of State Data Notification Laws, Foley & Lardner website.

Lawyers may be subject to ethics complaints related to privacy for failing to safeguard client information. Equally important, the EU Regulations impose privacy standards often far more rigorous than those in the U.S. - and which must be followed by companies with an international presence. See also Section re: Privacy & PII.

**Failure to Safeguard Customer Information** - In the wake of data breaches, the FTC has pursued enforcement actions against companies for in connection with deceptive or inadequate security practices. See e.g., Settlement With Online Tax Prep Service (8/2107)(finding that tax prep service failed to safeguard customers’ financial information in violation of Gramm_LeachBliley and exposed customers to risk by not requiring strong passwords), Settlement With Ashley Madison (12/2016)(complaint that dating service failed to protect 36 million users’ account and profile information in relation to a massive July 2015 data breach of their network, including falsely representing Trusted Security status and failing to honor "no delete policy.

**Cybersecurity Insurance:** Is cybersecurity insurance necessary and what types of cybersecurity losses are covered under business insurance policies? Certain types of damages may be excluded from your coverage. See e.g., P.F. Chang’s China Bistro, Inc. v. Federal Insurance Company, No. 15-cv-1322 (SMM), 2016 WL 3055111 (D. Ariz. May 31, 2016)(finding that cyber insurance policy covered $1.7 million for losses associated with data breach, but upholding insurer’s disclaimer of coverage for $2 million in fees and assessments that P.F. Changs that contractually agreed to reimburse to MasterCard as part of its services agreement); Columbia Casualty Insurance v. Cottage Health, Case 2:16-cv-3759 (C.D. Ca. 2016)(denying coverage where insured failed to comply with certain security measures required by insurer). Law firms are not immune from these limitations Moses Afonso v. CT Corporation, Docket 1-17-00157 (4/21/2017)(law firm seeking coverage for $700,000 in business losses resulting from ransomware attack and not covered by policy).

**Standing:** Those denied coverage under a cybersecurity policy clearly have standing to sue. But what about the victims of the breach - can they sue for invasion of privacy? The law is ever-evolving. See Privacy: Data & Biometric Information for detailed discussion on standing.
Other Issues: The cybersecurity environment is ever-changing with new legislation at state and federal level frequently introduced - not to mention enactment of laws worldwide which will govern companies engaged in business internationally.

Future Trends & Opportunities: Demand for lawyers with cybersecurity knowledge will increase over the next few years. Though biglaw has a lock representation of large financial institutes, small businesses (including solo and small law firms!) will need guidance as will consumers impacted by data breaches. We’ve only seen the tip of the iceberg with cybersecurity issues - hackers’ skills continue to increase and many companies will require legal risk assessment expertise to identify the fine line between making systems convenient to customers while ensuring adequate security. What’s more, we haven’t seen the full scope of damage since as many hackers may sit on information gathered for two or three years (the period when customers often install security protection) so the wave of litigation over cybersecurity breaches, along with applicable statutory deadlines and causation, is only just beginning.

BONUS - Lawyers & Cybersecurity

When handling personal information, lawyers must abide by the duty of competent representation cover by ABA Model Rule 1.1 and the duty of confidentiality defined by ABA Model Rule 1.6. In 2017, the ABA also released Formal Opinion 477, updating its earlier opinions on transmittal of confidential information over the Internet. Although the ABA continues to find that a lawyer may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct, the lawyer must take reasonable efforts to prevent inadvertent or unauthorized access, and further, take special security precautions when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security. Critically, compliance with ethics rules do not excuse attorneys from adhering to federal and state laws governing cybersecurity and data privacy.
DATA CENTER LAW

WHAT IS IT?
A data center is a facility that houses an organization’s IT operations and equipment, as well as where it stores, manages, and disseminates its data. A data center is similar to the cloud in that both are used to store data but the cloud stores data on a third-party platform accessible anywhere on the internet and a data center refers to the on-site, physical hardware such as servers and equipment used to store data. See Business Daily News. Data Center law encompasses legal issues unique to data centers, ranging from security and lease consideration to energy usage.

WHY NOW?
The demand for data centers has expanded with the growth of companies like Google, Amazon and Facebook that support billions of transactions and store massive amounts of user data. The transition from onsite storage to the cloud by banks, medical providers and law firms has also fueled the growth of new data centers. That’s because cloud service providers still need physical data centers to store all of the data and services made accessible through the cloud. The global data center market is predicted to expand from $6 billion in 2017 to $10 billion by the end of 2022, according to a recent study. Today’s data centers are massive facilities that consume large quantities of energy and house data that is vital to millions of transactions. Because of the costs involved in operating data centers, the enormous consequences of an outage or data loss, and the global nature of data, representation of data centers has evolved into a practice area primarily dominated by large, international law firms.

KEY LEGAL ISSUES:
Data center issues arise in two contexts: representation of the data center itself, or representation of companies that contract for space in shared data centers. Many of the issues below are relevant to both data center owners and customer:

Liability Issues: Data centers will want to restrict liability for outages (power, cooling, humidity, security) while customers often require assurance that these potential issues will not result in outages or data losses that can harm their business. There is potential for large claims to be brought against data center operators for loss of business or profits or data arising from outages. In one instance, frequent outages cost a data center a large customer, and as a result, the data center was forced to declare bankruptcy. See Oregon Data Center in Bankruptcy, Oregon Live (6/2016).

Energy costs: Data centers consume enormous amounts of power. The costs are substantial enough to prompt a data center owner in
Nevada to sue regulators and the state’s utilities over changes in solar energy pricing that lead to the data center being overcharged. See Switch Sues Over Solar Deal, Fortune (7/14/2016). Many of the companies that run large data centers -such as Amazon, Google and Facebook are environmentally conscious and favor renewable energy and may need legal assistance with renewable energy procurement, including advice on maximizing tax benefits. Energy costs are also subject to variation, and those centers that rely on fossil fuel as a power source may face higher costs in the future due to carbon tax or other changes in energy policy. A data center owner will want to take account of these costs in its contracts, and negotiate for provisions that allow the data center to pass on or at least share cost increases. Finally, all power systems are subject to outage, which in turn may impact data centers. This risk should be accounted for in contracts with customers or through insurance coverage.

**Regulatory and Security Issues** - Data centers must comply with strict regulatory obligations around protection of and/access to data and how they should be dealt with in your contracts with your customers, including in relation to data privacy and protection of data, fair use of data, interception of data or otherwise.

**Site Security** - Data center owners must ensure that the facility and site and secure - not just from land-based, physical intrusion or outside hackers, but also from threats in the air from overhead drones. See Is the Airspace Above Your Data Center Secure?, http://www.datacenterknowledge.com/archives/2016/03/14/drones-is-the-airspace-above-your-data-center-secure

**Intellectual Property** - Apparently, even the design of data centers has IP value - in February 2017, a federal judge refused to dismiss a lawsuit against Facebook alleging that the giant stole the design of one of its data centers from a British engineering company. See https://arstechnica.com/tech-policy/2017/02/did-facebook-steal-the-design-for-its-data-center-in-sweden/

---

**Future Trends & Opportunities:**

Many large law firms have already introduced data center practices that capitalize on multi-disciplinary skills - though small firm energy lawyers or real estate firms could carve out a sub-niche. Moreover, data centers themselves aren’t the only focus of this practice area; increasingly, smaller companies rely on 3rd party data centers to serve customers, and they too require representation. As the cloud continues grow, so too will data center law.
DIGITAL ASSETS IN ESTATE PLANNING AND SUCCESSION

WHAT IS IT?

Digital assets encompass communications, data, documents, photographs, intellectual property and other materials that are committed to digital format, confer a right of use and have an intrinsic or acquired value. Today, nearly everyone, irrespective of class or age owns some type of digital assets which include (1) accounts on or other sites for such as photo-sharing, genealogy research, online genetic testing services or fantasy sports; (2) blogs and publications; (3) email (whether housed locally or on a cloud-based service such as gmail), photos, video and other writings; (4) online businesses; (5) cloud-based storage and (6) financial assets, such as online bank accounts, credit card account and cryptocurrencies. Digital assets may be housed on a user’s local machine, or on third party platforms owned by third parties.

WHY NOW?

Increasingly, individuals of all ages and classes have digital assets. Five years ago, a McAfee Report found that average consumers value their digital assets at around $37,000; that number is likely to skyrocket over the next five to ten years. Yet many individuals fail to realize that unless they make arrangements for disposition of digital assets within their estate plans, the value will be lost to heirs and beneficiaries. The problems associated with transfer of digital assets is further complicated because of the involvement of third party hosts (e.g., Facebook, Gmail, etc...) which may have their own policies in place for transferring digital assets (much in the same way that Retirement Plans each have their own practices for designating beneficiaries). Many estate planning attorneys fail to inquire about clients’ digital assets or are unfamiliar with practices of individual platforms or new laws that apply to disposition of digital assets in estate planning.

Moreover, because digital asset disposition is so specialized, it can even be pursued as a stand-alone niche rather than bundled as part of an estate planning practice. In other words, an attorney interested in the digital asset field can gain expertise and serve as a consultant to other law firms, and potentially advise some of the emerging companies that hold online assets (e.g., Everplans.com, Safebeyond.com) on compliance with applicable data storage and digital asset requirements.

State of Law: Currently, there is some guidance for practitioners on estate planning for digital assets. A site called DeadSocial.org (note the site was moving at the time of publication) contains “death guides” for five top sites with information on designating legacy contacts, and accessing content post-death. (Each individual site contains the information but it’s handily aggregated at Dead Social).
The National Conference of Commissioners on Uniform State Laws also devised the Revised Uniform Fiduciary Access to Digital Assets Act (UFADAA), which has been adopted by 21 states as of this writing (states listed at above link). This Act extends the traditional power of a fiduciary to manage tangible property to include management of a person’s digital assets. The act allows fiduciaries to manage digital property like computer files, web domains, and virtual currency, but restricts a fiduciary’s access to electronic communications such as email, text messages, and accounts unless the original user consented in a will, trust, power of attorney, or other record.

In states that have not adopted the UFADAA, fiduciaries generally have much more limited authority over digital assets. Heirs may be unable to access password protected accounts, or may be locked out by platform-specific terms of service which generally prohibit access to an account by anyone by the original user.

**KEY LEGAL ISSUES:**

**Conflict between UFADDA and Other Federal Laws:** Although the UFADDA allows for designation of a fiduciary, some uncertainty remains over whether the fiduciary’s access to a user’s account, even if authorized potentially violates the Electronic Communications Protection Act (ECPA) which prohibits interception of communications by third parties.

Does UFADDA Void End User Agreements? In most cases, the company that issues the user’s electronic account retains control of the content - for example, Apple retains a user’s itunes collection after his death. UFADDA gives authorized fiduciaries control of the decedent’s account - but this control may conflict with user agreements and terms of service. This potential conflict remains unresolved. Likewise, it is unclear whether a fiduciary can continue to operate or use a decedent’s account (which may also violate a platform’s terms of service) - or if the fiduciary’s activities are limited to winding down and memorializing the account and preserving the content.

**Other Matters:**

- How should digital assets be valued for estate planning purposes?
- What kind of guidance should estate planning lawyers provide on digital assets?
- How should account passwords be handled to avoid opening them to public scrutiny as in a will?

**Future Trends & Opportunities:** The demand for attorneys with digital asset expertise will continue to grow. Not only will clients increasingly keep assets online, but the types of assets that can be reduced to digital format will grow.
DRONE LAW

WHAT IS IT?

A drone, also known as an unmanned aerial vehicle (UAV), is an aircraft without a human pilot aboard. There are three main categories of drones: commercial (or enterprise) - which are used for business, consumer (or recreational) which are used for educational or non-business purposes and government drones which includes military and regulatory compliance applications. Over the past decade, drones have gone from being a mysterious, sci-fi object associated with criminal activity or surveillance to mainstream. Today, commercial drones infiltrate virtually every industry - agriculture, environmental protection, energy, building inspections and even shark-watching on Australian beaches. And drones are also likely to be used for mainstream retail deliveries on the not-to-distant horizon. Meanwhile, consumers are now purchasing drones for recreational purposes - either to fly for fun or for aerial photography.

WHY NOW?

The drone market is experiencing explosive growth with sales expected to surge from $8.5 billion in 2016 to $12 billion in 2021, according to Business Insider, July 2017.

Several reasons account for this growth. Improved drone technology has driven rapid adoption of drone technologies in the enterprise sector and declining costs for good-quality consumer drones makes them more accessible to, and popular with the general public. New manufacturers have also been enticed by the bullish drone market, thus increasing competition and further decreasing costs. Regulatory action by the FAA also spurred growth; in 2015, the FAA issued hundreds of exemptions for commercial drones, and put a framework in place for consumer drones. See Business Insider, July 2017.

KEY LEGAL ISSUES:

Already, drones have been the subject personal injury and unlawful surveillance actions. See e.g., JRuproctlaw.com (list of drone cases) But these cases are not particularly noteworthy but for the fact that
they involve drones. By contrast, the issues below relate to evolving legal issues related to drones:

**Federal Authority Over Drones** - The federal government has exclusive authority over regulation of “transit through navigable airspace (49 U.S.C. §40103), which has been delegated to the FAA and is one source of the FAA’s regulatory power over drones. The second source of FAA regulatory power over drones is found in the Modernization and Reform Act of 2012 which empowered the FAA to issue regulations specific to drones. Exercising this authority, in 2015, the FAA created the Section 333 exemption for operation of civil, commercial drone operators for small aircraft 55 pounds or less. Once the exemption is granted, the drone operator is still subject to certain requirements: the aircraft must be registered, operated by a pilot in command with FAA airman certificate, cannot go above 400 feet and must remain within the line of pilot’s site of site and must have a visual observer as part of operations. In 2016, the FAA offered a second option to the Section 333 exemption for commercial drones -- a Part 107 waiver which subjects operators to similar requirements, with some minor exceptions summarized in this [FAA Fact Sheet](#) on Exemptions & Waivers.

Model aircraft used for fun are subject to separate (and less onerous) FAA requirements (e.g., they do not require a licensed pilot for operation but height and line of vision rules still apply). In addition, effective May 2018, model aircraft owners must register with the FAA, a requirement under the National Defense Authorization Act, signed into law in December 2017. The Act overrides an earlier federal court decision that vacated an earlier FAA rule requiring registration of model aircraft, after finding that the FAA lacked authority to regulate drones for personal use. See [Time Magazine](#), December 12, 2017.

**Preemption Issues**: In some instances, the FAA rules clash with local laws restricting drone operation, thus raising preemption questions. Singer v. City of Newton, CA No. 17-0071 (D. Ma. 9/21/2017), the most recent case speaking to preemption involved a challenge to a City local ordinance which required drone operators to register their aircraft with the City, prohibited pilotless aircraft flight below an altitude of 400 feet over any private property without the express permission of the property owner and prohibited drones from public airspace within the town impermissibly. The court found that the City’s regulations encroached on the FAA’s authority over drones in navigable airspace and accordingly, was preempted. See also [FAA Fact Sheet](#) (expressing need for uniform regulatory framework for operation of drones and suggesting that state laws conflicting with FAA’s overarching authority may be preempted).

**Privacy** - Currently, FAA regulations do not regulate drone privacy - a deficiency that the Electronic Privacy Information Center (EPIC) unsuccessfully attempted to challenge. See EPIC v. FAA, 821 F.3d 39 (2016)(dismissing EPIC challenge as untimely). To date, at least
31 states have laws that address drone use and privacy, generally limiting drone use in private spaces, crowds and government buildings. See Esteban Morales, Update on Drone Regulation, Law 360 (10/2016). In California, an individuals who uses a drone to record visual images via a drone is liable for invasion of privacy, Texas prohibits use of drones for surveillance, and Kansas makes it illegal to stalk someone with a drone.

**Trespass** - Trespass claims are likely survive preemption by federal law. See e.g., Integration of Drones Into Domestic Airspace, CRS Report (2013)(describing common law grounds for protection of airspace from trespass). In Boggs v. Meredith, 3:16-cv-0006 WD Ky 3/21/2017, a drone owner flew his aircraft over his neighbor’s property, who promptly shot it down. The drone owner sued, arguing that he had perated his drone in accordance with federal law and did not violate the landowner’s expectation of privacy. The drone owner also sought recovery of $1500 for damage to his drone. The court dismissed the suit, finding that the claim for damage to the drone was a “garden variety tort claim” and did not involve a federal question. The Boggs ruling suggests that claims for trespass, nuisance involving drones will continue to be resolved under state law. Indeed, in 2015, a California small claims judge ordered a property owner to reimburse a drone operator $750 for shooting down his drone. See Man Wins Lawsuit After Drone Shot Down, Motherboard (6/28/2017).

**Equal Protection** - in Flores v. Texas, 5:16-cv-00130 (August 2016), a Mexican resident of a town along the Texas-Mexico border challenge constitutionality of a Texas law that allows drone surveillance along the Texas Mexico border. The resident arguing that the law violated his equal protection rights by reducing privacy rights for those living along the border.

**Future Trends & Opportunities:** Preemption will continue to be a key issue with regard to drone regulation as the industry grows. Large national companies would prefer a single national law to a patchwork of state requirements, but at the same time, federal regulations may complicate compliance for hobbyists. At the same time, matters like personal privacy, crime, trespass and zoning have traditionally been within the purview of states and localities which will have an increased interest in protecting residents as drones become more prevalent.
Drone Law – Update

Preemption - In July 2018, the FAA issued a Press Release to clarify the role of federal and state/local regulation of drones. The Press Release reaffirms the FAA’s power to regulate aviation space and air traffic control and prohibits cities and municipalities from adopting their own regulation governing operation of drones while recognizing that they "may generally determine the location of aircraft landing sites through their land use powers."

Trespass and Tort Laws - National Conference on Commissioners on Uniform State Laws: Tort Law Relating to Drones proposed a law that would define “aerial trespass” for purposes of tort liability. Specifically, the draft law provides that:

“"A person operating an unmanned aircraft is liable to a landowner or lessee for per se trespass when the person, without consent, intentionally causes the unmanned aircraft to enter into the airspace below 200 feet above the surface of land or below 200 feet above improvements built upon the surface of the land.”

Exclusions to the doctrine include conduct protected by the First Amendment,” public safety efforts, or operations by employees/contractors with a “valid easement, right of way or license.”

Not surprisingly, neither commercial drone operators (including Amazon as expressed here) nor the FAA have endorsed the draft which would potentially exposure drone operators to liability for trespass and could potentially encroach on the FAA’s regulatory powers over drones as the FAA expressed in comments on the draft regulations here.
E-ACCESSIBILITY LAW

WHAT IS IT?
E-Accessibility refers to a set of procedures and practices designed to make Internet content accessible to individuals with disabilities. For example, text can be made accessible to people who are blind by providing an audio option, and streaming content can be made accessible to people who are deaf by adding closed captioning. The World Wide Web Consortium has developed Web Content Accessibility Guidelines, a set of best practices for making websites accessible.

WHY NOW?
E-accessibility suits began in 2000, when Bank of America became the first entity to settle a web-accessibility lawsuit. Safeway and Charles Schwab soon followed suit. In 2008, Target paid $6 million to settle a class-action suit brought by the National Federation of the Blind, and nearly $4 million more to cover the plaintiffs’ attorney fees and other costs.

These trends are not surprising. As the Justice Department has explained, “[t]he Internet has become an essential tool for many Americans and, when accessible, provides individuals with disabilities great independence.” Thus, e-accessibility suits continue to rise, with 260 actions filed in federal court in 2016. See generally, National Review, July 27, 2017.

Many suits are brought against retailers and the hospitality industry. More recently, however, litigation has been brought against universities on the grounds that the free online courses they offer aren’t captioned for deaf users, and against ride-sharing services because their smartphone apps lack text-to-speech capability for blind users. See LA Times, 6/11/2016; also Section on Sharing Economy.

Although the ADA covers e-accessibility claims, rules have not yet been enacted to provide guidance to businesses so that they can avoid violations. Without clear rules, lawsuits are expected to increase. See National Review (11/27/2017).

KEY LEGAL ISSUES:
Below are some of the legal issues that are currently brewing or may soon arise related to e-accessibility:

Websites As Public Accommodations: Recently, disability rights groups have brought a number of lawsuits under the Americans with Disabilities Act (“ADA”) against websites they deem insufficiently accessible. The ADA “public accommodations” from discriminating against people with disabilities, and requires these entities to provide “reasonable accommodations” for these individuals. See ADA Regulations. Disability rights groups have argued that websites are public accommodations, and the
Department of Justice and some courts have agreed. See e.g., https://arstechnica.com/tech-policy/2015/04/9th-circuit-rules-netflix-isnt-subject-to-disability-law/ (noting that, although the Ninth Circuit determined in an unpublished opinion that Netflix was not a public accommodation, the District of Massachusetts held that it was). Most famously, advocates for deaf people obtained a consent decree in 2012 that required Netflix to provide closed captions for all of its videos. See Netflix Consent Decree.

Other E-Accessibility Questions:

- Do certain color combinations violate the ADA because they confound the colorblind?
- Are certain layouts inaccessible if they’re confusing to users with a limited field of vision?
- Do the accessibility requirements apply only to the websites themselves, or do they also apply to Web content, such as advertising on a third party’s website?
- Will website hosts be responsible for the compliance of third-party sites?
- Must archived Web content be revised to comply?
- What type of e-accessibility is required for mobile apps?
- Do temporary technical bugs in an otherwise compliant website constitute a violation?

Future Trends & Opportunities: So far, Web accessibility lawsuits have concerned the vision- and hearing-impaired, but future cases could be brought on behalf of plaintiffs diagnosed with dyslexia, ADD/ADHD, narcolepsy, cognitive impairments, paralysis and many other conditions.
FIRST AMENDMENT & ONLINE DEFAMATION

WHAT IS IT?

The First Amendment protects free speech and expression. Defamation is injury to a person’s character, fame or reputation by false and malicious statements, whether oral (i.e., slander) or in writing (i.e., libel). Defamation laws must balance the protection of a person’s “good” reputation with the First Amendment protections afforded to the speaker.

WHY NOW?

Today, the Internet and social media have become the equivalent of the “modern public square.” Packingham v. North Carolina, 137 S. Ct. 1730 (2017). Most obviously, with the advent of the Internet in the 1990s, “publication” (essential to a claim of defamation) of materials to an audience of millions occurs in an instant. As a result, more platforms exist for publication of defamatory material than in the pre-Internet era. But legislative policy also accounts for the rise of defamation claims. In light of the Age of the Internet, Congress adopted the Communications Decency Act of 1996 (“CDA” at 47 U.S.C. § 230, et. seq.), which included a safe harbor provision (the “Good Samaritan privilege”) for Internet Service Providers (ISPs), granting immunity for defamatory content posted by third parties or anonymous posters through their online services. The protection for ISPs enables them to host anonymous and potentially defamatory content without regard to liability, thus emboldening posters and leading to an increase of potentially defamatory commentary.

KEY LEGAL ISSUES:

Jurisdiction - There are often state jurisdictional issues, as victim and perpetrator are often in different states, if not different countries. There is a split in the jurisdictions whether or not you can sue the defamatory speaker in your home state. See e.g., Baldwin v. Fischer-Smith, 315 S.W.3d 389 (Mo. 2010), Missouri Court of Appeals held that there was personal jurisdiction over the web-postings directed towards the plaintiff in Missouri; although the court noted that the state court had broad jurisdictional views on communication with the forum state, quoting, “if you pick a fight in Missouri, you can reasonably expect to settle it here.” (quoting Revell v. Lidov, 317 F.3d 467, 476 (5th Cir. 2002). The Baldwin Court also noted that the Supreme Court declined to consider jurisdictional issues in an internet setting in Young v. New Haven Advocate, 315 F.3d 256, 262-64 (4th Cir. 2002), cert. den’d, 538 U.S. 1035 (2003).
However, in Others First, Inc. v. Better Business Bureau, 2014 WL 6455682, 2:14-cv-12066-GCS-PJK (E.D. Mich. 2014), the court granted defendant’s motion to dismiss based upon lack of personal jurisdiction because simply posting something on a website that damages a Michigan resident, even if Michigan residency is known, is insufficient. Curiously, within a few weeks, Others First filed an identical lawsuit in St. Louis, Missouri, which was dismissed on summary judgment for, inter alia, failure to make a prima facie case of defamation, finding that all of the “injurious” comments were either truthful or protected opinion based speech. Others First, Inc. v. The Better Business Bureau of Greater St. Louis, Inc., 105 F.Supp.2d 923 (E.D. Mo. 2015), aff’d, No. 15-2184 (8th Cir. 2016). Similarly, the Texas Supreme Court In re Doe a/k/a “Trooper,” No. 13-0073 (Sup. Ct. 2014), where a blogger posted defamatory comments about the Reynolds & Reynolds company, the court ultimately dismissed the lower court rulings for lack of personal jurisdiction because the defendant did not have minimum contacts; the court did not want Texas to become “the world’s inspector general.” In Yelp, Inc. v. Hadeed Carpet Cleaning, Inc., No. 140242 (Sup. Ct. 2015), the Virginia Supreme Court overturned the lower court’s rulings holding that there was no jurisdiction under the state’s long-arm statutes because Yelp was located in California and data relating to the alleged remarks against Hadeed was stored in that state.

Communications Decency Act Immunity: Internet Service Providers (ISPs) do not have to police their sites and remove libelous or infringing content, and no legal obligation to remove libelous or privacy infringing materials when notified (although for most government associated social media sites, those administrators forewarn that all posts are subject to scrutiny, at time pre-approval, and removal). This rule precludes a plaintiff from bringing defamation suit against the ISPs. See, e.g., S.C. v. Dirty World, LLC, Case No. 11-CV-00392-DW, 2012 U.S. Dist. LEXIS 118297 (W.D. Mo. 2012), the CDA granted immunity to Dirty World from plaintiff’s defamation and other claims relating to posts submitted by a third-party user; and Jones v. Dirty World Entm’t Recordings LLC, 755 F.3d 398 (6th Cir. 2014) (holding the CDA granted immunity and ISPs could not be found to have materially contributed to the defamatory content of posted statements simply because the posts were selected by them for publication or because they decided not to remove the posts). However, one recent much-watched case suggests a shift away from the previously near iron-clad immunity afforded by the CDA. See Hassell v. Bird, 2016 WL 3163296 (Cal. App. Ct. 6/7/2016), cert granted Hassell v. Ava Bird/Yelp, 2017 Cal. LEXIS 1418 (Cal. 2/14/2017). There an attorney sued a former client for posting a negative Yelp review in which the client complained of the attorney improperly overcharging for copies and phone calls. The client never appeared, and the court awarded $557,918.75 and ordered Yelp (which had not been a party to the suit) to remove the
reviews. On appeal to the California Supreme court (decision pending), Yelp argued that the court’s order to remove content effectively makes Yelp liable for information provided by users in violation of the CDA. For in-depth discussion of CDA trends, see Eric Goldman, *10 Most Important Section 230 Rulings*, Tulane J. Law & Tech (2017).

**Anonymity & Online Reviews:** Typically, the plaintiff must seek pre-litigation discovery, and enforce third-party subpoenas against an ISP to unmask the anonymous defamatory speaker. There are a number of tests employed throughout the courts, including the “good faith standard” (i.e., showing good faith effort to locate the individual and comply with service of process requirements) or “motion to dismiss” standard (i.e., plaintiff set forth a prima facie case that would withstand a motion to dismiss). However, the most prevalent test is the *Dendrite-Cahill* test, or a modified version (which emerged from (*Dendrite Int’l Inc. v. Doe*, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001); and *Doe v. Cahill*, 884 A.2d 451 (Del. 2005) (condensed version)), which test is favorable to anonymous commentators and discourages “sue-first, ask questions later” litigation strategy. The test is, essentially:

- Efforts to notify the anonymous commenter and allow a reasonable time for him or her to respond;
- Identify the exact statements made by the commenter;
- Set forth a prima facie cause of action, presenting evidence to win the case barring any defenses or additional evidence presented by the commenter;
- Set forth sufficient evidence for each element of its defamation claim; and,
- The court must balance the speaker's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous commenter's identity.

The Maryland Supreme Court in Independent Newspapers, *Inc. v. Brodie*, No. 63, Sept. Term, 2008 (2009) (where bloggers posted that the Brodie owned Dunkin’ Donuts shop was one “of the most dirty and unsanitary-looking food-service places I have seen”) ruled that the bloggers could not be unmasked. The Brodie court set forth a summary analysis of the progeny of the *Dendrite* case and adopted its test, holding that it most appropriately balances a speaker's constitutional right to anonymous Internet speech with a plaintiff’s right to seek judicial redress from defamatory remarks; the court noted that the “good faith basis” or “motion to dismiss” thresholds were too low a bar that would inhibit the use of the Internet as a marketplace of ideas, but that the summary judgment standard was too high a bar that would undermine personal accountability and the search for the truth.
A recent decision by the California State *Yelp Inc. v. Superior Court Orange County*, online at, (November 2017), the court held that companies have a right to litigate on behalf of users to withhold information, but nevertheless, required Yelp to disclose the identity of a user who posted a negative review of an accounting firm. For more discussion, see *Anonymity for Review Sites Slipping Away*, Reuters.com. For other issues related to anonymous speech and discovery of identity of speaker, see section Social Media for the discussion on mixed application of an ISPs defense to third-party subpoenas under the Federal Stored Communications Act (18 U.S.C. §2701) and/or as “remote computing service” (18 U.S.C. § 2711(2)).

**Defamation Issues** - To make a claim for a defamatory statement, a number of issues must be considered, including (1) whether the content identified the plaintiff, so that the intended audience would know that the post targeted the plaintiff; (2) whether the content was an assertion of fact or opinion and (3) whether the the assertions are true. Even defamation suits involving highly damaging claims - such as a resort's inclusion on a list of a travel website's list of Ten Dirtiest Hotels or President Trump's tweet calling a political advisor a “major loser” who had “begged” him for a job - have been dismissed because courts deemed the comments pure opinion and therefore protected. See e.g., *Seaton v. Tripadvisor*, No. 12-6122 (6th Cir. 2013)(dismissing defamation suit against Trip Advisor by hotel described as “dirtiest”); *NY Appeals Court Dismisses Defamation Suit Against Trump*, NY Herald (12/14/2017). On the other hand, defamation suits challenging claims regarding factual matters are more likely to survive. This was true in a recent, widely reported case involving two newlyweds who engaged in a concerted smear campaign on social media disparaging their wedding photographer for failing to timely deliver their wedding photos. A jury found the couple’s remarks defamatory and awarded a $1 million verdict after determining that the remarks destroyed the photographer’s business. See *Polito v. Moldovan*, DC 15-03069, 193 Jud. Dist. TX (2017); also *NBC News* coverage (August 17, 2017). As relevant to lawyers, there are several instances where they have prevailed in defamation actions against former clients for negative reviews. See *Hassell v. Bird*, supra., *Court Upholds Verdict for Lawyer*, BNA.com (3/27/2014)(affirming defamation award in favor of attorney against client who posted reviews that she was a crook); see also *Blake v. Ann-Marie Giustibelli*, (Florida District Court 2016)(affirming defamation award by lawyer against former client for negative review which alleged that lawyer overbilled and lied to the court).

Although a viable defamation claim traditionally requires a showing of damages, in the age of the internet, there are some instances which the court permits the plaintiff to proceed without showing actual damage. See, e.g., *W.J.A. v. D.A.*, A-0762-09T3 (NJ Superior Ct., App. Div., 2010), aff’d, A-77-10 (NJ Sup. Ct. 2012), the court ruled a defamation suit over online accusations of child sexual abuse could still proceed, even though the plaintiff could not show
he was harmed. In Obsidian Fin. Group, LLC v. Cox, 740 F.3d 1284 (9th Cir. 2014) held, inter alia, that liability for a defamatory blog post involving a matter of public concern cannot be imposed without proof of fault and actual damages.

**Journalists & Media Protection** The Cox case, supra, is notable for several reasons, but for in the context of this subject, let’s focus on the first amendment protections: the lower court (U.S.D.C. District of Oregon), ruled that Cox, an internet blogger, was not a journalist and therefore not protected by Oregon’s media shield laws, although it later clarified that it did not categorically exclude all blogs but only Cox’s blog because she offered plaintiff’s removal of negative posts for a $2,500.00 fee. Ultimately, jury awarded plaintiffs $2.5 million against Cox; and Cox was unsuccessful in petitioning the court to grant a retrial, with the court ruling that private figure plaintiffs do not have to establish negligence or actual malice to hold non-media defendants liable in defamation suits arising out of speech not on a matter of public concern (see Cox, No. 3:11-cv-57-HZ (D.C. Oregon, 2012)). However, the Ninth Circuit affirmed in part and overturned in part, partially vacated the judgment awarding compensatory damages, and ordered a new trial. The Court held, although the Supreme Court has not decided the issue, almost every U.S. Court of Appeals has determined that First Amendment protections apply equally to both institutional press and individual speakers; Judge Andrew Hurwitz opined that there are a host of big rulings, including Citizens United v. FEC, that reject the notion that the institutional press has First Amendment advantages that individual speakers do not. The Court ruled that the blog post was a matter of public concern, even if the plaintiffs were private individuals, and, as such, bloggers posting libelous entries about private citizens concerning public matters can only be sued if they’re negligent (the same as news media), and the case was remanded for a new trial on Cox’s negligence. The Supreme Court denied the writ of certiorari (Cox, 134 S. Ct. 2680).

**Harassment & Bullying** - Sometimes, online posts stray from the realm of defamation and are more properly characterized as Cyber harassment or Cyberbulling (which is discussed in its own section). Please note that 37 states have cyberstalking laws; 41 states have cyberharassment laws; and there is a federal stalking statute which covers cyberstalking).

**Laws That Protect Online Speech** - Strategic Lawsuit Against Public Participation or a "SLAPP suit," is a retaliatory lawsuit by businesses or executives against individuals posting messages on review sites, internet financial message boards, or in online chat rooms; the claims are usually but not always based on a libel claim, against discussion on a public issue or controversy in an attempt to silence critics and intimidate other internet users to keep criticisms to themselves. There are 27 states, the District of Columbia and Guam with Anti-SLAPP statutory protections in place which
facilitate prompt resolution of such claims, however there is no uniformity in the scope and levels of protection between the states.

The Consumer Fairness Protection Act of 2016 is a more recent legislative initiative designed designed to protect consumers who use ratings sites from legal action by the subjects of their reviews. The Act takes aim at the practice employed by many companies of including non-disparagement clauses in terms of service for products and services to silence consumers from posting damaging online reviews. The Consumer Fairness Review Act of 2016 prohibits companies from including clauses contracts that restrict the ability of a consumer to communicate regarding the goods or services offered or purchased. The FTC enforces the Act. See FTC Statement re: Consumer Fairness Review Act.

Future Trends & Opportunities: Over time, the pendulum will continue to swing between First Amendment freedom and defamation claims. For example, with the Internet no longer in its nascency, some have argued that the immunity afforded to ISPs and content hosts under the CDA is no longer necessary. Any changes to the CDA - and it is likely there will be at least some in the near future - will change the landscape of online defamation claims. The scope of clients in need of online First Amendment representation will continue to grow, including individual bloggers, businesses impacted by online reviews and online websites and businesses.
GENETIC COUNSELING AND DISCRIMINATION

WHAT IS IT?

Genetic testing is a type of medical test on blood and other tissue to identify changes in chromosomes, genes, or proteins. There are thousands of tests available, and more are being developed. Genetic testing is used for several reasons, such as finding: genetic diseases in embryos or unborn babies; whether a person is predisposed to a genetic disease or condition before symptoms appear; whether a person will pass on a genetic disease to their children; diagnosing a disease after symptoms appear; or, even determining the optimal type or dose of medicine for a person. Since the 1980s, there has been a strong push for genetic testing, both for individual and general research purposes (e.g., the Human Genome Project).

The possibility of genetic discrimination is a major concern for those considering (and/or declining) genetic testing. Genetic discrimination occurs from unfair and/or differential treatment by an employer or insurance company because a person has or is perceived to have a gene mutation that causes or increases the risk of an inherited disorder (e.g., breast cancer, Alzheimer’s, heart disease, etc.).

WHY NOW?

Genetic testing has been around for some time, but has grown increasingly pervasive as costs decline, technology improves and the scope of identifiable conditions increases. Likewise, while the potential for genetic discrimination has been recognized for some time, the law is evolving.

Two decades ago, the Americans With Disabilities Act (ADA) was the primary federal statutory vehicle for pursuit of genetic discrimination claims. See, e.g., EEOC v. Burlington N. & S.F.R. Co., Case No.: 2:02-cv-00456-CNC (E.D. Wis.)($3.8 million settlement in suit against Burlington North for firing employee who refused to submit to genetic test for carpal tunnel syndrome in violation of ADA. On September 25, 2008, the ADA Amendments Act of 2008 was signed into law in an effort to expand the application of “disability,” but the law did not address the issue of genetic discrimination or discrimination based on risk of future impairment. Unfortunately, the courts have not ruled on the application of the ADA in the specific context of genetic discrimination, as the courts have traditionally not been receptive of the EEOC genetic discrimination challenges under the ADA. But, see, gen., Chadam v. Palo Alto Unified Sch. Dist., 2016 U.S. App.
In 2008, the Genetic Information Nondiscrimination Act of 2008 (Pub.L. 110–233, 122 Stat. 881, enacted May 21, 2008, (“GINA”)) was enacted to prohibit some types of genetic discrimination in most employment scenarios. GINA, however, does not protect persons from genetic discrimination in every circumstance. For example, neither provision applies to schools or financial institutions/lenders when an employer has less than 15 employees or to U.S. military personnel or persons receiving health benefits through the Veterans Health Administration or Indian Health Service. Also, Title I applies only to health insurance, not other types of insurance such as life insurance, disability or long-term care insurance. Moreover, Title I does not extend to people who are already affected by a genetic condition (i.e., showing symptoms or clinical manifestations of a condition).

The EEOC is the main enforcing agency of GINA legislation. Beginning in 2013, the EEOC has filed a number of GINA and ADA lawsuits specifically for genetic discrimination (as discussed herein below). On May 17, 2016, the EEOC issued final rules to amend the regulations on employer wellness programs for both GINA (note: regulations at https://www.federalregister.gov/documents/2016/05/17/2016-11557/genetic-information-nondiscrimination-act)) and the ADA issued final rules that same day as well. (note: regulations at https://www.federalregister.gov/documents/2016/05/17/2016-11558/regulations-under-the-americans-with-disabilities-act), which regulations took effect on January 1, 2017. Specifically, the amended regulations removed the ADA safe harbor provisions; programs must be voluntary in nature; collection of disability-related information and medical exams must comply with ERISA and HIPPA protections; employers cannot deny insurance for non-participation; and, employers cannot retaliate for non-participation. Additionally, the new regulations cover spousal participation in such programs, and employers may not ask employees or covered dependents to agree to permit the sale of their genetic information in exchange for participation. However, the future of the new rules is uncertain in light of a judicial remand. See 2017 U.S. Dist. LEXIS 133650 (D.D.C. August 22, 2017)(remand of the rules to the EEOC for reconsideration and development of a reasoned explanation in a timely manner for the connection between the voluntariness of the program and the 30% cap (see id. at *54), but allowing them to remain in effect pending resolution).

KEY LEGAL ISSUES:

**EEOC Actions** - Under GINA, Employers must tell health care providers not to question family medical history during post-offer or fitness-for-duty examinations, with exceptions under its Safe Harbor provision: (a) inadvertent receipt of genetic information or pursuant to the FMLA; (b) employee receives voluntary health or genetic services from employer offers; or (c) genetic information is obtained from “commercially and publicly available” sources (e.g., newspapers, books and public websites); and, all acquired genetic information must be kept confidential subject to certain narrow
exceptions. It is the EEOC’s opinion that the ADA’s broad definition of disability (42 U.S.C. §12102(2)(c)), combined with the widely-held views of genetic determinism, widespread genetic illiteracy, and the breadth of GINA’s statutory definition of “genetic information”, ensures that GINA Title II and ADA claims will be brought concurrently when individuals believe themselves to be the victims of genetic discrimination in employment contexts.

On May 7, 2013, the EEOC filed its first lawsuit under Title II of GINA (EEOC v. Fabricut, Inc., Case No.: 13-CV-248-CVE-PJC (N.D. Okla.) concurrently with a consent decree to settle the lawsuit, with Fabricut paying $50,000.00 in damages, for GINA violations by requesting family medical history in its post-offer medical exams and Americans with Disabilities Act (ADA) violations for disability labeling.

A few days later, on May 16, 2013, the EEOC filed another suit (EEOC v. Founders Pavilion, Inc. d/b/a Founders Pavilion, Case No. 6:13-cv-06250 (W.D.N.Y)) asserting its first “systemic discrimination” under GINA (a “pattern or practice, policy, or class case where the alleged discrimination has a broad impact on an industry, profession, company or geographic area.”) for requesting family medical history as part of its post-offer, pre-employment medical exams of applicants and during annual follow-up medical exams for employees, as well as violations under the ADA and Title VII. The Founders case settled on January 13, 2014, with Founders paying $110,400.00 to settle the GINA claims and $259,600.00 to settle the ADA and Title VII allegations.

On September 30, 2013, the EEOC filed suit against the Abatti Group and its subsidiaries for GINA and ADA violations (EEOC v. All Star Seed dba Eight Star Commodities, Green Touch Fertilizer, & Allstar Seed Co.; La Valle Sabbia, Inc. dba Eight Star Equip. & Eight Star Logistics; & Abatti dba Abatti Cos., Case No. CV13-07196 JAK (AJWx) (C.D. Ca.) for requiring job applicants to answer unlawful medical and genetic information inquiries; the case settled on November 14, 2014 with the three companies (Abatti, All Star Seed and La Valle Sabbia Inc.) paying $187,500.00.

On September 9, 2014, EEOC filed suit against Cummins Power for GINA and ADA violations relating to fitness-for-duty examinations (EEOC v. Cummins Power Generation, Civil Action 0:14-cv-03408-SRN-SER (D. Minn.)). During the litigation, Cummins Power claimed third-party vendors that drafted the violative forms were indispensable parties, but the court granted the EEOC’s motion to dismiss this defense (EEOC v. Cummins Power Generation, Inc., 313 F.R.D. 93 (D. Minn. 2015) (“Cummins, as the employer, is liable for a violation of the ADA or GINA related to [the release] ‘regardless of whether third parties [were] also in­volved in the discrimination”)). The Cummins Power case ultimately settled on May 6, 2016, with Cummins Power paying $87,500.00 and furnishing other equitable relief.

Several days later, on September 17, 2014, the EEOC filed suit against BNV Home Care Agency, Inc. (EEOC v. BNV Home Care Agency, Inc., Case No. 14-CV-5441-JBW-RML (E.D.N.Y), which settled on October 31, 2016 with BNV paying $125,000.00 to current employees that were asked impressionable genetic questions on the health assessment form.
In 2014, EEOC also filed three (3) unsuccessful consecutive suits regarding wellness program violations under, primarily, the ADA. First, on August 20, 2014, EEOC v. Orion Energy Sys., Case No. 1:14CV01019 (E.D. Wis.) was filed challenging an employer wellness program solely under the ADA. On cross-summary judgment motions, the district court denied the EEOC’s motion and partially granted Orion’s motion, in so far as the court held that although the ADA safe harbor provisions did not apply, Orion’s wellness program was voluntary, but that there remained questions of fact on EEOC’s retaliation claims, and the case was scheduled for trial (see id., 208 F. Supp. 3d 989 (E.D. Wis. September 19, 2016). Ultimately, the case settled with, inter alia, Orion paying $100,000.00 in damages (see id., Case No. 1:14CV01019 (E.D. Wis. April 4, 2017).

Second, on September 30, 2014, EEOC v. Flambeau, Inc., Case No. 3:14-00638 (W.D. Wis.) also filed solely under the ADA. On cross-summary judgment motions, the court denied the EEOC’s motion and granted Flambeau’s motion, thereby dismissing the EEOC’s complaint, holding that the wellness program fell under the ADA’s safe harbor provisions; the Seventh Circuit Court of Appeals subsequently affirmed the decision (note: it was a case of first impression). See id., 131 F. Supp. 3d 849, 856 (W.D. Wis. Dec. 31, 2015), aff’d, 846 F.3d 941 (7th Cir. January 25, 2017).

Last, on October 27, 2014, EEOC v. Honeywell Int’l, Inc., Case No.: 0:14-04517 (D. Minn.) was filed under both the ADA and GINA (with the latter in reference to forcing spouses to undergo genetic screening for health insurance coverage), but it was voluntarily dismissed after the court denied the EEOC’s TRO request without addressing the merits of the case (see id., 2014 U.S. Dist. LEXIS 157945, at *14 (D. Minn. Nov. 6, 2014)).

On August 13, 2015, the EEOC filed suit against Bedford Weaving for GINA and ADA violations for medical assessments (EEOC v. Bedford Weaving, Inc., Civil Action No. 6:15-CV-00027-NKM) (W.D. Va.); it appears that the suit is still pending.


On March 26, 2016, EEOC v. Grisham Farm Prods., Inc., Case No. 6:16-CV-3105 MDH (W.D. Mo.) was filed, claiming violations of the ADA and GINA for health history screenings as a prerequisite to job applications. The court granted EEOC’s motion for judgment on the pleadings, holding that Grisham Farms liable on all EEOC accounts, and ordering implantation of policies to prevent future discrimination and payment of $10,000.00 in damages (see id., 191 F. Supp. 3d 994 (W.D. Mo. June 8, 2016).

Federal Lawsuits - Lowe v. Atlas Logistics Group Retail Servs. Atlanta, LLC, Case No. 1:13-CV-2425-AT (N.D. Ga.) was a case of first impression for the nation for application of GINA between an employer and employee. Employees sued their employer for GINA violations after conducting DNA testing in connection with disciplinary investigations. The United States District Court Northern District of Georgia granted the employee’s motion for summary judgment, holding the employer in violation of
GINA (see id., 102 F. Supp. 3d 1360 (N.D. Ga. May 5, 2015)). The court held a trial on damages, and on June 22, 2015, the first jury verdict based upon GINA violations was issued, awarding $2.2 million to the plaintiffs ($475,000 in emotional distress damages and $1.75 million in punitive damages based on the employer’s reckless indifference to their federally protected rights); but, the court reduced the verdict in its August 5, 2015 Order, and judgment was entered in the amount of $600,000.00 in total (equally for both plaintiffs), plus post-judgment interest (see, e.g., gen., id., 2015 U.S. Dist. LEXIS 178275 (N.D. Ga. September 28, 2015).

Affordable Care Act Issues - This law provides additional protection by prohibiting health insurance discrimination based on pre-existing conditions, including genetic conditions. ACA provides additional protections for patients with genetic diseases by establishing that certain health insurers may only vary premiums based on a few specified factors such as age or geographic area, thereby prohibiting the adjustment of premiums because of medical conditions.

The Health Insurance Portability and Accountability Act of 1996 (HIPPA) - One part of Title I of GINA required HIPPA amendments (privacy requirements for health information), and the modifications made in 2013 state that genetic information is considered to be health information; therefore, it cannot be used by health insurers to make any decisions about health insurance benefits, eligibility for benefits, or the calculation of premiums under a health plan.

Ancillary State Laws: Several state laws have been enacted to supplement the federal legislation, although the laws vary widely in scope, applicability and the amount of protection provided; GINA offers minimum protections and does not pre-empt state laws with stricter protections. The earliest state laws focused on particular genetic conditions (e.g., the sickle-cell trait (FL and LA) or the hemoglobin trait (NC). In 1981, NJ enacted a statute (later broadened) to prohibit discrimination in employment based on an "atypical hereditary cellular or blood trait," and a NY law prohibited employers from denying equal employment opportunities based on "unique genetic disorders." In 1991, Wisconsin was the first state to prevent wholesale discrimination based on genetic tests. At present, 48 states (note: not Miss. and Wash.) and D.C. have passed laws preventing genetic discrimination in health insurance providers. Some states have passed laws to prohibit this discrimination in "other insurers" (e.g., in 2011, "California Genetic Information Nondiscrimination Act" (CalGINA), was passed and extended protections even further to prohibit genetic discrimination in emergency medical services, housing, mortgage lending, education, and other state-funded programs). At present, 17 states have additional laws restricting the use of genetic information in determining coverage for life insurance, 17 states for disability insurance, and eight states for long-term care insurance. Currently, 35 states and D.C. prevent genetic discrimination in employment. For example, OR state law prohibits employers from using genetic information to distinguish between or discriminate against applicants and employees and prohibits employers from subjecting applicants and employees to genetic testing. A recently enacted TX law prohibits employers, labor organizations, licensing agencies, and
employment agencies from discriminating against any individual on the basis of the results of a genetic test or because of the individual's refusal to submit to genetic testing.

Future Trends & Opportunities: When GINA legislation was introduced, genetic testing was still in the realm of academic science. Since the 2000s, next generation sequencing for genetic analysis has become a commercial product (like 23andme and AncestryDNA), and genetic testing is becoming more common place in the universal endeavor to achieve personalized medicine. GINA is a strong law an essential first step against genetic discrimination and misuse of medical information, but it isn't perfect. In March 2017, the Preserving Employee Wellness Programs Act (HR 1313) was introduced to addresses the right of an employer to request and use an employee's health and genetic information as it pertains to enrollment in employer-sponsored wellness programs and disbursement of incentives for such programs. The bill in its current form exempts workplace wellness programs from: (1) limitations under the Americans with Disabilities Act of 1990 on medical examinations and inquiries of employees, (2) the prohibition on collecting genetic information in connection with issuing health insurance, and (3) limitations under the Genetic Information Nondiscrimination Act of 2008 on collecting the genetic information of employees or family members of employees. This exemption applies to workplace wellness programs that comply with limits on rewards for employees participating in the program. HR 1313 passed the House Education and the Workforce Committee on March 8, 2017, and the committees on Energy and Commerce, and Ways and Means are considering the bill; it is expected to be included as part of the efforts in ACA replacement.
INTERNET OF THINGS

WHAT IS IT?

According to Wikipedia, the Internet of Things (IoT) encompasses the network of physical devices, vehicles, home appliances and other items embedded with software that enables these “things” to connect to the internet and collect and exchange data. It is estimated that the IoT will exceed 6.4 billion devices by the end of 2016, and as many as 30 billion objects by 2020. The wearables market alone is expected to be worth $25 billion by 2009, while home security market will be valued at $53 billion by 2022. See Motley Fool (11/25/17). Because IoT devices automate processes (such as turning on household appliances) and track and share data (think, Fitbits), some of the legal issues that these technologies raise intersect with two other topics covered - data & privacy law and robot law. But as discussed, there are other issues unique to IoT.

WHY NOW?

The law of IoT is a hot legal issue for a number of reasons. For starters, IoT encompasses range of diverse devices: medical devices, home security systems, children’s technology and voice-activation home tools like Alexa and Google Home. The technology isn’t expensive and many consumers have quickly integrated these devices into their everyday lives. This widespread use likewise means that there are many opportunities for something to go wrong - raising questions about which entity is to blame: the device developer? the user? or other third party technology that links the two?

Because the law is not clear, IoT doesn’t just raise legal issues, but policy questions. In 2013, the FTC convened a workshop on security and privacy in IoT (online at which lead to publication of a report recommending best practices. See A few months ago, the Department of Commerce convened a working group to develop procedures by which IoT providers provide security updates to customers. See Department of Commerce Draft Doc on IoT. Even Congress has also taken a stab at increasing regulation of IoT with proposed legislation to require that IoT devices purchased by the U.S. government meet certain cybersecurity standards. See https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices.

KEY LEGAL ISSUES

Data Security - Any digital device with an internet connection is vulnerable to hacking. As IoT devices become more widespread, they have become a target for hackers. Perhaps to facilitate
connection, security on IoT devices is less than ideal – few IoT devices encrypt data they collect and users employ weak access credentials. IoT manufacturers’ lax security is already the subject of at least one lawsuit, Toyota, Ford, and General Motors. Cahen v. Toyota Motor Corp., No. 3:15-cv-01104 (N.D. Cal. Mar. 10, 2015)(alleging that defendants sold unsafe cars because their Internet connectivity creates vulnerability to hackers, who could then gain control of the cars’ operation). Moreover, when it comes to cybersecurity, what is the appropriate mechanism for assigning liability? Should manufacturers be strictly liable for damages flowing from an inherently insecure design, and if so, to what extent? Or should careless users bear the blame for IoT security breaches.

Privacy Issues - Because IoT technologies collect data, there’s a potential for privacy violations if data isn’t sufficiently secured and anonymized, or if users aren’t aware that data is being collected to begin with. Two recent examples: In NP v. Standard Innovation, Case No. 1:16-cv-8655 (ND 2016), plaintiffs settled a class action lawsuit for privacy violations against a “smart” vibrator company for $3.75 million, where the company failed to disclose to its customers that it collected data on usage and other information that would allow for identification of the customer and further, was susceptible to hacking. See Chicago Tribune, (6/9/2016).

And pending at the 7th Circuit (No. 16-3766) is an appeal of a ruling in Now Naperville v. Smart Meter Awareness, 114 F.Supp. 3d 606 (ND Ill. 2015), where the court dismissed plaintiffs’ claims that data collection by smart meters installed by the utility in their homes violated their privacy rights under the Fourth Amendment and the Illinois Constitution.

Consumer Protection/False Advertising Like any consumer product, IoT devices are subject to consumer protection laws. Using its authority under Section 5 of the FTC Act, the FTC has initiated enforcement actions against three different IoT companies. The FTC alleged that each company’s representations about the first-rate security of their respective systems were deceptive when a hacker readily accessed one of the systems and posted 700 IP addresses to the company website, while in another case (involving among other things, baby monitors), the company failed to address obvious and easy to fix security flaws. See e.g., FTC Website (1/2017). States have also pursued false advertising claims under state law: in May 2017, the New York AG’s office settled a case with a company that provides insecure wireless doors and padlocks which had been marketed as secure.

Discovery Issues - Already, lawyers have found opportunities to make use of IoT data in both civil and criminal cases. In one case in Canada, Fitbit data was obtained and will be used to show that the plaintiff’s activity levels deteriorated from her baseline after an accident. See In another case, a woman’s claim that she had been asleep when an intruder entered her house was disproved by Fitbit data which showed that she was awake and walking around her house. http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/

COPPA Issues - In October 2017, the FTC released guidance on the applicability of the Child Online Privacy Protection Act (COPPA) - which requires websites or online services to obtain parental consent before collecting personal information from children under 13 - applies to voice recordings. The new FTC regulations raise
issues about whether COPPA may apply to voice activated IoT devices, particularly those aimed at children. See https://www.lexology.com/library/detail.aspx?g=52e44267-270f-4503-8e98-e948cd3afe46 Concerns about children’s use of IoT is not hypothetical in light of a recent study that found that most IoT toys for kids can be easily hacked. See Smart Toys Let Attackers Listen to Your Kids, Tech Dirt (11/04/2017)

Discovery Data from wearables and other IoT devices can be subpoenaed during discovery. In a recent case, Amazon moved to quash a subpoena seeking recordings from an Amazon echo, asserting that the responses are protected First Amendment speech (ultimately, the defendant consented to release of the data) See Evidence from Wearable Tech, ABA Journal (3/17/17). Even when data is made available, there may be obstacles to admissibility since IoT devices raise questions regarding (1) the reliability of the data, (2) what the data actually means (since different devices store raw data differently), and (3) whether the chain of custody was preserved.

Compliance Issues - Counsel for companies that develop IoT devices must be familiar with the above issues to help their clients comply with applicable law. The FTC has a useful interactive, online guide to help developers of mobile health apps identify applicable laws. Compliance is further complicated because as discussed above, IoT devices are subject not only to federal law but also to different state laws.

Future Opportunities & Trends:

Expect new rules to evolve over IoT and perhaps for Congress to step in. IoT providers will have a difficult time complying with different state consumer protection laws without some universal guidance. At some point, applicable privacy laws - such as HIPAA for health care devices - may be expanded to cover IoT devices In addition, attorneys will continue to push the envelope on the extent to which IoT companies may be held liable for privacy or security breaches, even where there is no harm. One final emerging issue is whether de-anonymization of data is sufficient to truly protect privacy, and how to strike a balance between permitting providers to aggregate data to improve a product and allowing users to retain full control and ownership of data they generate. The FCC’s potential end to net neutrality is also expected to impact IoT - which requires substantial bandwidth - and could give rise to anti-trust actions as ISPs compete to offer exclusive service to specific providers in exchange for increased payments, or attempt to tie internet service to specific IoT apps.
LAWYERS AND INTERNET SCAMS

WHAT IS IT?
Fraudulent check scams are nothing new, but such an operation has become much more widespread and sophisticated through the Internet. Lawyers and law firms have become targeted groups, and are, surprisingly, vulnerable to becoming entangled in fraudulent check schemes. There are three common Internet scams which specifically target lawyers: e-mail based client request (usually asking the lawyer to deposit a settlement check which is counterfeit), ransomware (where computer network is infected with malicious software) and impersonation of an existing client.

WHY NOW?
Hacker attacks are on the rise and will continue with scammers becoming more sophisticated.

KEY LEGAL ISSUES:
Third-Party Claims and/or Disciplinary Action: When an attorney and/or firm losses funds based upon Internet scams, it can result in third-party lawsuits and disciplinary actions. All attorneys are subject to Rules of Professional Conduct, which imposes an ongoing duty to not disclose client confidential information; and to maintain, properly manage and safeguard client funds; and have specific rules to the administration of IOLA/IOLTA accounts. In New York, the wiring of client’s money without authorization is prima facie evidence of the breach of the standard of care in a legal malpractice action. Typically, an attorney who misappropriates or converts client funds is presumptively unfit to practice law, and, absent mitigating circumstances and even unintentional misappropriation or repayment of all the money can result in discipline. Moreover, liability may be imputed on other partners of the firm because they should have been aware of how the firm escrow account was being handled, and are fully responsible for its misuse.

No Bank Liability: All the liability rests upon the attorney and/or firm; a bank has none of the liability for not recognizing a check to be counterfeit (however, under the terms of the banking agreement, the lawyer and/or firm is liable to make the bank whole for the unqualified funds). The New York Court of Appeals in Greenberg, Trager & Herbst, LLP v. HSBC Bank USA, 17 N.Y.3d 565 (2011), held that a law firm is in the best position to guard against the risk of a counterfeit check by knowing its client. Id. at 582.

Business Owner’s Policy: Some attorneys/firms maintain Business Owner Policies that provide coverage resulting directly from forgery or alteration of checks, drafts, promissory notes, etc.; however, it is unlikely that this type of policy will coverage in an email scam because the check received is a counterfeit. Alt seems to be a necessary ingredient of forgery that some alteration or fabrication of an instrument or some part of it is made by which its
meaning or language is changed, or whereby a new operation is
given to it; and, if what has been written upon or erased from an
instrument has no tendency to produce this result, or to mislead any
person, it is not a forgery or alteration. United States Nat'l Bank v.
National Park Bank, 13 N.Y.S. 411, 413 (1st Dept. 1891), aff'd 129
payee's name is the classic alteration. It can with modern technology
be effected by forging a check rather than by altering an original
check ...@ but a forgery was the A duplication of the entire check
(that is, forgery of the check deposited with the presenting bank),
rather than just physical alteration of the payee's name on the
original check.@); and Bank of Am., N.A. v. Mazon State Bank, 500
F. Supp. 2d 803 (ND Ill 2007) (Aif the check were >altered,= that
would mean that the original check ... signed and mailed was
deposited after the payee line was somehow changed (via chemical
washing or some other method) ... If the check were forged, by
contrast, it might mean that the perpetrator of the fraud >used
sophisticated copying technology to produce a copy that was
identical in every respect to the original check . . . except for an
undetectable change of the payee's name).

Professional Liability Policy Duty to Defend: At times, an
attorney and/or firm can, at least, invoke its malpractice policy to
help defend against cases where the bank is seeking a
reimbursement from the attorney and/or firm. A determining factor
in lawyer-insurer litigation surrounding scams is often whether or
not the activity was related to the firm’s “professional” services. See,
e.g., Attorneys Liab. Protection Soc., Inc. v. Whittington Law
Assocs., PLLC, 961 F.Supp.2d 367 (D. N.H. 2013) (no duty to
defend for losses due to “Nigerian check scam” because of the
exclusion that there would be no coverage for any claim involving
“conversion” or “misappropriation” of “client or trust account funds
or property, or funds or property of any other person held or
controlled by an Insured in any capacity or under any authority”); Bradford & Bradford, P.A. v. Attorneys Liab. Prot. Soc’y, Inc., No. 09-
cv-2981, 2010 U.S. Dist. LEXIS 111923 (D.S.C. 2010) (losses due to
Nigerian Check Scam did not arise from provision of professional
services and no duty to defend against lawsuit by bank to recover
funds lost due to trust account fraud); and Fid. Bank v. Stapleton,
Compare Lombardi, Walsh, Wakeman, Harrison, Amodeo &
1291 (3d Dept. 2011) (insurance company required to defend law
firm against lawsuit by bank for lost funds because the handling a
client’s funds is part of the legal services provided, even when the
client is an imposter); and Yudin & Yudin, PLLC v Liberty Inter’l
2012) (same).

Professional Liability Policy Duty to Indemnify: Sometimes, an attorney and/or firm can recoup some of its loss
through its malpractice insurance because the lost funds came from
another client’s account or the IOLTA account; however, in the last
decades, some insurance companies are placing exclusions in the
policies to prevent coverage. See Nardella Chong, P.A. v. Medmarc
Cas. Ins. Co., 642 F.3d 941 (11th Cir. 2011) (the court ordered
indemnification for the firm’s “short fall” because the A[m]isuse of a
client's funds (even though deposited in a bank account physically controlled by the attorney) is one of the most serious offenses a lawyer can commit; management of these funds held in trust for clients constitutes a professional service and since the court concluded that Chong's management of its trust account constituted a professional service, the policy covers claims alleging negligence in this management, including those that could have been asserted here); O'Brien & Wolf, L.L.P. v. Liberty Ins. Underwriters, Inc., Civil No. 11-3748, 2012 U.S. Dist. LEXIS 109089 (D. Minn. 2012) (the court ordered indemnification because the damages sought by the insured are of a known and undisputed amount - the $110,500 erroneously transferred out of the client trust account minus the insured=s deductible and Stark & Knoll Co., L.P.A. v. ProAssurance Cas. Co., 2013 U.S. Dist. LEXIS 50326(N.D. Oh. 2013) (the policy covered "services rendered by an Insured as a provider of legal services in a lawyer-client relationship" or "activities of an Insured as a trustee... or in any other fiduciary capacity" and the court held that this definition applied to potential claims against the lawyer by "existing clients whose funds were improperly disposed of" when the bank seized accounts to cover its losses). Compare Fleet Nat'l Bank v. Wolsky, 2006 Mass. Super. LEXIS 688 (Mass. Super. Ct. 2006) (no duty to indemnify because the receipt, endorsing and depositing a check, and dispersing the proceeds does not constitute the rendering of legal services for purposes of the attorney's professional liability policy).

Cybersecurity Insurance Policies: Cybersecurity insurance will pay expenses associated with a computer network hack, such as the cost of extortion or ransom; loss of income; cost of hiring forensic investigators; and liability protection and defense costs, including bringing on a legal team to advise the firm of its potential risk. However, as this is a new area of insurance, there is not a significant amount of case law on the issues that may arise. See, e.g., gen., Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., 103 F. Supp. 3d 1297 (D. Utah 2015) (this was the first coverage decision with respect to a stand-alone cyber insurance policy and the court interpreted the policy similar to any other general liability policy, ultimately holding no duty to defend; the company alleged knowledge, willfulness, and malice in its action against the insureds because the company alleged that the insureds knowingly withheld data and refused to turn it over until the company met certain demands); and Columbia Cas. Co. v. Cottage Health Sys., No. 2:15-cv-03432, 2015 U.S. Dist. LEXIS 93456 (C.D. Cal. 2015) (although the case was dismissed for ADR, the insurer contendted that the insured failed to adhere to the basic security practices (e.g., file transfer protocol (FTP) settings, the application of patches, computer network assessments, and detecting network intrusions), and the failure to do so was the cause of the data breach and subsequent loss, which was an exclusion under the policy for a failure to follow minimum required practices).
Future Trends & Opportunities:

Internet schemes will continue to grow and become more sophisticated in targeting preferred groups, such as attorneys. There is some, but not much recourse for the victim. At times, authorities have been able to arrest and prosecute perpetrators (see, e.g., U.S. v. Adindu, No. 16-cr-00575 (S.D.N.Y. 2016), but it is not often that stolen funds are recouped. Indeed, malpractice insurance policies will be tailored to include exclusions for this type of mismanagement; and, cyber security policies have their own pitfalls. Attorneys must be vigilant.
LGBTQ ISSUES

WHAT IS IT?

LGBT is an acronym for the lesbian, gay, bisexual and transgender community. The initialism of LGBT is intended to emphasize sexual and gender identity diversity, and the title is ever-evolving to be as inclusive as possible to represent non-heterosexual or non-cisgender persons. Currently, the most common reference is LGBTQ (Q is for queer or questioning), but the most inclusive title is LGGBBTTQQIAAPP (lesbian, gay, genderqueer, bisexual, bigender, transgender, trans, queer, questioning, intersex, asexual, agender, pansexual and polyamorous); the appropriate identification will continue to adapt as more gender and sexual identities are recognized.

WHY NOW?

More than any other factor, the rise of the LGBT movement and influence is largely attributable to changing American attitudes. A recent Pew Research Report (6/13/2017) found that 63% of Americans said in 2016 that homosexuality should be accepted by society, compared with 51% in 2006. LGBT adults recognize the change in attitudes with 92 percent acknowledging society's increased acceptance. As a result, today's younger generations are less fearful of identifying as LGBT. Today, young adults, ages 18 to 36, are by far the most likely to identify as LGBT (7.3%). By contrast, much smaller shares of those ages 37 to 51 (3.2%), 52 to 70 (2.4%) and 71 and older (1.4%) say they are LGBT, according to Gallup.

These more tolerant attitudes have lead to great advances for the LGBTQ community for federal and state recognized rights and protection over the past 15 years. Still, political climates are fickle and some predict that many of these gains will be lost with the Trump Administration now in office. See How Trump Made 2017 A Horrific Year for LGBT Rights & Worst Is To Come, Daily Beast (12/20/2017).

KEY LEGAL ISSUES:

Hate Crimes - On October 22, 2009, Congress finally passed the Matthew Shepard and James Byrd Jr. Hate Crimes Prevention Act (the Shepard-Byrd Hate Crimes Prevention Act), which was signed by President Obama on October 28, 2009, expanding the U.S. federal hate-crime law to include crimes motivated by a victim’s actual or perceived gender, sexual orientation, gender identity, or disability, as well as authorize the Federal Bureau of Investigations (FBI) to collect statistics on these types of hate crimes. The first convictions under the Act occurred in 2011 for two (2) individuals involved in running a car containing five Hispanic men off the road; the first plead guilty and the second was found guilty at trial. See U.S. v. Maybee, 2011 U.S. Dist. LEXIS 77302 (W.D. Ark., July 15, 2011).
2011), aff’d, 687 F.3d 1026 (8th Cir. Aug. 6, 2012), rehearing den’d, 2012 U.S. App. LEXIS 18671 (8th Cir. Sept. 5, 2012), cert. den’d, 133 S. Ct. 556 (Oct. 29, 2012). See also id., 2013 U.S. Dist. LEXIS 106357 (W.D. Ark. Apr. 17, 2013) (post-conviction proceedings and magistrate’s recommendations). In 2016, the Act was first used to prosecute an individual for a transgender-based crime (because Mississippi did not have a statute to protect gender-identity victims, the United States Department of Justice (DOJ), Southern District of Mississippi, brought federal charges); the defendant pled guilty and was sentenced to 49 years in prison and $20,000.00 for the murder of a transgender teen. See DOJ Press Release.

LGBT & Military - Congress passed The Don't Ask, Don't Tell Repeal Act of 2010 (H.R. 2965, S. 4023) that established a process for ending the Don't ask, don't tell (DADT) policy (10 U.S.C. § 654), thus allowing gays, lesbians, and bisexuals to serve openly in the United States Armed Forces; implementation of repeal was completed 60 days later, so that DADT was no longer policy as of September 20, 2011. On June 30, 2016, following a study conducted by the RAND Corp.), Obama Administration Department of Defense (DoD) Secretary, Ashton B. Carter, issued a Directive-type Memorandum ("DTM") announcing that transgender Americans can openly serve in the U.S. military (approximately 2,450 transgender servicemen) and the government would cover medical costs of service members to undergo gender transitions; the DOD issued an Implementation Handbook on September 30, 2016. On August 28, 2017, the Trump Administration officially announced its new policy to reverse the Obama-era edict, and directed, inter alia, to halt the use of federal funds to pay for sexual reassignment surgeries and medications, except in cases where it is deemed necessary to protect the health of an individual who has already begun the transition, and to discharge of all transgender service members starting in March 2018 (82 FR 41319) at Homeland Security Memo, White House Press Office (8/25/2017)). On September 14, 2017, Trump Administration DoD Secretary James Mattis issued a memorandum establishing an interim policy until the directives take effect with no immediate effect on individual service members pending the implementation plan. Currently, litigation is pending on 82 FR 41319, with the district courts temporarily blocking parts of the Order, and the status of this issue is unclear (at least, until the Supreme Court undoubtedly will hear the cases). See, e.g., Doe v. Trump, Case No. 17-1597-CKK, 2017 U.S. Dist. LEXIS 178892 (D. D.C. Oct. 30, 2017) (court granted partial preliminary injunction against sections 1(b) and 2(a) of the directive, and partially granted the Administration’s motion to dismiss, dismissing plaintiff’s claims based upon the Sex Reassignment Surgery Directive and estoppel claims). On November 21, 2017, the DOJ filed an appeal of the Doe decision to the D.C. Court of Appeals (D.C. Cir.) (note: on November 28, 2017, the Senate confirmed (50-48) White House and Trump legal adviser, Gregory Katsas, to that bench). See also id., Case No. 17-1597-CKK (D.D.C. Nov. 27, 2017) (clarification order requiring the military to allow openly serving transgender recruits starting on January 1, 2018 per the status quo preceding 82 FR 41319); an appeal was filed by the DOJ on December 6, 2017 to the D.C. Court of Appeals. In the interim, on November 14, 2017, the military’s first gender reassignment surgery was conducted at a private facility and covered by the military’s health coverage because it was deemed medically necessary; the
DoD stated that the active-duty service member was granted a 82 FR 41319 waiver by the director of the Defense Health Agency because the service member had already begun sex-reassignment course treatment. See also Stone v. Trump, Case No. MJG-17-2459, 2017 U.S. Dist. LEXIS 192183 (D. Md. Nov. 21, 2017) (the court granted a preliminary injunction on 82 FR 41319 in its entirety (including prohibition on gender reassignment surgery), and partially granted the Administration’s motion to dismiss, dismissing a claim of violation of 10 U.S.C. § 1074 (military entitlement to medical and dental care in military treatment facilities), but permitting claims for violations under 5th Amendment Due Process and 14th Amendment Substantive Due Process); it is anticipated that the DOJ will file an appeal. See also Karlinsky v. Trump, Case No. C17-0129-MJP, 2017 U.S. Dist. LEXIS 191911 (W.D. Wash., Nov. 20, 2017) (litigation challenging constitutionality of 82 FR 41319, court denied Administration’s motion for a stay pending outcome of Doe case and appeal); and id., Case No. C17-0129-MJP, 2017 U.S. Dist. LEXIS 194406 (W.D. Wash. Nov. 27, 2017) (granting motion by State of Washington to intervene under Fed. R. Civ. Pro. 24).

Same Sex Marriage - The United States Supreme Court recently issued several landmark decisions for the LGBTQ community. In U.S. v. Windsor, 133 S. Ct. 2675 (June 26, 2013), the Court affirmed the Second Circuit decision and ruled (5-4) that Section 3 of the Defense of Marriage Act (DOMA) (P.L. 104–199 (enacted Sept. 21, 1996) 1 U.S.C. § 7 & 28 U.S.C. § 1738C), which provided that the term “spouse” only applied to marriages between a man and woman, was unconstitutional under the Due Process Clause of the Fifth Amendment. See also id., 833 F. Supp. 2d 394 (S.D.N.Y. June 6, 2012), aff’d, 699 F.3d 169 (2d Cir. Oct. 18, 2012) (case was challenge the IRS denial of federal estate tax exemption for surviving spouses by same-sex surviving spouse). Consequently, committed same-sex couples that were legally married in their own states can receive federal protections. Curiously enough, famed-plaintiff Edith Windsor just died at the age of 88 on September 19, 2017. On the same day as the Windsor decision, the Court issued a decision (also 5-4) on Hollingsworth v. Perry, 133 S. Ct. 2652 (June 26, 2013), which struck down the appeal regarding the constitutionality of California’s Proposition 8 (state ban on same-sex marriage) for lack of standing; thus, the lower court’s decision that Prop 8 was unconstitutional was valid. See also id., 725 F.3d 1140 (9th Cir. Aug. 6, 2013) (dismissing appeal for lack of jurisdiction in accordance the Supreme Court’s opinion of June 26, 2013). The Hollingsworth case, essentially, marked the end of Prop 8’s five-year journey and removed legal battles for California same-sex couples wishing to marry, but did not directly affect other states. Then, in Obergefell v. Hodges, 135 S. Ct. 2584 (June 26, 2015), the Court ruled (5-4) that Section 2 of DOMA, which gave legal relief to any state from recognizing same-sex marriages performed in other jurisdictions, was unconstitutional under the 14th Amendment; thus, granting the “fundamental right to marry” for same-sex couples (#LoveWins). The Obergefell decision was, ultimately, the consolidation of six cases: Obergefell v. Wymyslo, Case No. 1:13-cv-501 (S.D. Ohio); Henry v. Himes, Case No. 1:14-cv-129 (S.D. Ohio); Tanco v. Haslam, Case No. 3:13-cv-01159 (M.D. Tenn.); Deboer v. Snyder, Case No. 12-cv-10285 (E.D. Mich.); Bourke v. Beshear, Case No. 3:13-cv-750-H (W.D. Ky.); and Love v. Beshear, Case No.: 3:13-cv-750-H (W.D. Ky.); and ultimately rendered the last remaining provision of
DOMA unenforceable. The Obergefell decision also overturned the Baker v. Nelson decision, in which the U.S. Supreme Court had dismissed an appeal from the Minnesota Supreme Court ruling that a state law limited marriage to persons of opposite sex did not violate the U.S. Constitution, “for want of a substantial federal question.” See id., 291 Minn. 310 (Oct. 15, 1971), app. dismissed, 409 U.S. 810 (Oct. 10, 1972). Following, the Court in Pavan v. Smith, 137 S. Ct. 2075 (June 26, 2017) ruled that the Arkansas statute was unconstitutional to the extent that it did not permit same-sex couples to be listed on birth certificates in violation of Obergefell. See also, id., 2017 Ark. 284 (Oct. 19, 2017) (which directed the circuit court to award declaratory and injunctive relief as necessary to ensure that same-sex spouses are afforded the same right as opposite-sex spouses to be listed on a child’s birth certificate in Arkansas, which will implement the U.S. Supreme Court mandate without an impermissible rewriting of the statutes).

Most recently, on Monday, December 4, 2017, the U.S. Supreme Court denied the petition for writ of certiorari from the Texas Supreme Court, which revived a lawsuit that sought to eliminate benefits offered to same-sex spouses of the City of Houston employees by addressing an interlocutory appeal from the court of appeal’s vacatur of the trial court’s orders denying a plea to the jurisdiction and granting a temporary injunction prohibiting the Mayor from distributing government-subsidized benefits to gay spouses of city employees. The Texas Supreme Court ruled that under Obergefell and Pavan, the rights to a marriage license did not automatically entitle same-sex couples to spousal insurance benefits (i.e., no established right), and remanded the case to the trial court, with both parties being entitled to a full and fair opportunity to litigate their positions and declining to instruct the trial court on how to construe Obergefell on remand. See Pidgeon v. Turner, Case No. 15-0688, 2017 Tex. LEXIS 654 (June 30, 2017), cert. den’d, Case No.: 17-424 (Dec. 4, 2017). It is likely that the issue of same-sex benefits will have to be litigated fully and presented to the U.S.

were infringed by a law compelling statements of fact with which the objectors could not, and did not profess to, disagree; Hurley v. Irish-American Gay, 515 U.S. 557 (June 19, 1995) (cannot compel association; and First Amendment is violated when anti-discrimination laws are applied in a peculiar way to burden speech); and Boy Scouts of Am. v. Dale, 530 U.S. 640 (June 28, 2000) (constitutional right to ban gays because the BSA’s opposition to homosexuality as part of its “expressive message”) (note: the BSA permitted membership of gay youths starting on January 1, 2014, and permitted membership of transgender youths on January 30, 2017). Accord Glickman v. Wileman Bros. & Elliott, 521 U.S. 457, 469-70 n.13 (June 25, 1997) (“do not compel any person to engage in any actual or symbolic speech”). The state of Colorado has some setbacks in its factual position in the Masterpiece case. First, when the underlying incident took place (July 2012), Colorado refused to recognize same-sex marriages or civil unions (see Colo. Rev. Stat. § 14-2-104(1)(b) (2014)); Colorado only issued same-sex marriage licenses starting in October 2014 after a federal court rulings against the state. In addition, it is reported that the state has applied its public accommodations law in a disparate manner; Robert P. George and Sherif Girgis pointed out in the New York Times, “three times the state [Colorado] has declined to force pro-gay bakers to provide a Christian patron with a cake they could not in conscience create given their own convictions on sexuality and marriage. Colorado was right to recognize their First Amendment right against compelled speech. It’s wrong to deny Jack Phillips that same right.” See NYT, 12/4/2017.). The Supreme Court’s Masterpiece decision will be issued before the end of June 2018 and will set the tone for dozens of ongoing cases involving the clash between conservative religious beliefs and support for the LGBT community.

Employment Discrimination - Currently, only federal employees are guaranteed protection for sex- or gender-based discrimination pursuant to the Office of Personnel Management (OPM) interpretation of the Windsor and Obergefell decisions, and Presidential Executive Orders (EO). There are no similar federal protections for non-federal or private-sector employees. The Employment Non-Discrimination Act ( ENDA) has been introduced unsuccessfully in nearly every Congress since 1994; the Senate passed the legislation for the first time in 2013, but it failed to make it to the president’s desk. An increasing number of states have enacted laws to provide protections, but it is not uniform.

Federal Employees: On June 28, 2013, U.S. Office of Personnel Management (OPM) issued a memorandum, Guidance on the Extension of Benefits to Married Gay and Lesbian Federal Employees, Annuities, and Their Families, which states, “... (OPM) will now be able to extend benefits to Federal employees and annuitants who have legally married a spouse of the same sex.” (see also https://www.opm.gov/faqs/topic/benefitsforlgbt/index.aspx). Such federal benefits include, for example, the Federal Employee Health Benefit Program, the Federal Employee Group Life Insurance Program, the Federal Employee Dental and Vision Insurance Program, and the Federal Long Term Care Insurance Program.
In 1995, President Clinton signed EO 12968, which included, for the first time, sexual orientation in the non-discrimination language as part of the criteria for the issuance of security clearances. In 1998, President Clinton signed EO 13087, which amended President’ Nixon’s EO 11478 (1969) prohibiting discrimination in the competitive service of the federal civilian workforce, to include sexual orientation discrimination. On July 21, 2014, President Obama signed EO 13672, which further amended EO 11478 to include “gender identity” as well as amended President Johnson’s EO 11246 (1965) punishing discrimination by federal government contractors and sub-contractors, to include “sexual orientation and gender identity;” this became enforceable by the Department of Labor (41 CFR Parts 60-1, 60-2, 60-4, and 60-50).

Non-federal and private-sector employees: No federal law explicitly forbids private-sector discrimination based on sexual orientation, and Title VII of the Civil Rights Act of 1964 does not mention orientation or gender identity. The U.S. Supreme Court has held that Title VII’s prohibition on sex discrimination in the workplace also offers protection to employees who don't conform to traditional sex stereotypes. See, e.g., Oncale v. Sundowner Offshore Servs., 523 U.S. 75 (1998) (Title VII prohibits same-sex harassment); and Price Waterhouse v. Hopkins, 490 U.S. 228 (1989) (Title VII prohibits discrimination based on an employee’s non-conformance to traditional sex stereotypes (e.g., assumptions and/or expectations about how persons of a certain sex should dress, behave, etc.). Consequently, an increasing number of federal courts interpret this to mean that LGBTQ discrimination is forbidden under Title VII, but the holdings are split across the nation. Compare, e.g., Evans v. Georgia Reg’l Hosp., 850 F.3d 1248 (11th Cir. 2017), pet. for reh’g en banc filed (Mar. 31, 2017) (Title VII prohibits gender-nonconformity discrimination (which applies to transgender individuals), but does not prohibit employment discrimination based on sexual orientation (i.e., homosexuality)); and Chavez v. Credit Nation Auto Sales, LLC, 641 Fed. Appx. 883 (11th Cir. 2016); Anonymous v. Omnicom Grp., Inc., 852 F.3d 195 (2d Cir. 2017) (reversed order dismissing an HIV-positive gay man’s employment-discrimination suit because Price Waterhouse permits claims of sex stereotyping (note: the court stopped short of holding sexual orientation is protected)); and Hively v. Ivy Tech Cmty. College of Ind., 853 F.3d 339 (7th Cir. 2017) (Title VII prohibits employment discrimination based on sexual orientation); and Muhammad v. Caterpillar Inc., 767 F.3d 694 (7th Cir. 2014), as amended on denial of reh’g (Oct. 16, 2014) (Title VII does not include sexual orientation-related discrimination claims). See also, e.g., Baker v. Aetna Life Ins., et al., 228 F. Supp. 3d 764 (N.D. Tex. 2017) (Title VII sex discrimination for denial of employer-provided health insurance plan for costs associated with surgery related to gender transition); EEOC v. Scott Med. Health Ctr., P.C., 217 F. Supp. 3d 834 (W.D. Pa. 2016) (Title VII's "because of sex" provision prohibits discrimination on the basis of sexual orientation).
Equal Employment Opportunities Commission (EEOC): The EEOC explicitly holds that while Title VII does not explicitly include sexual orientation or gender identity, such discrimination is illegal (see: EEOC Summary, EEOC Enforcement Protections. See also, e.g., Macy v. Dep’t of Justice, EEOC Appeal No. 0120120821 (April 20, 2012) (transgender discrimination is sex discrimination in violation of Title VII because it involves non-conformance with gender norms and stereotypes, or based on a plain interpretation of the statutory language prohibiting discrimination because of sex); Lusardi v. Dep't of the Army, EEOC Appeal No. 0120133395 (March 27, 2015) (Title VII is violated where an employer denies an employee equal access to a common restroom corresponding to the employee’s gender identity, or harasses an employee because of a gender transition, such as by intentionally and persistently failing to use the name and gender pronoun corresponding to the employee’s gender identity as communicated to management and employees); and Baldwin v. Dep't of Trans., EEOC Appeal No. 0120133080 (July 15, 2015) (sexual orientation discrimination under Title VII).

DOJ: On December 18, 2014, Attorney General Eric Holder issued a memorandum, which stated that the DOJ interpreted “sex” discrimination as including gender identity. On October 4, 2017, Attorney General Jeff Sessions issued a new memorandum, stating that the interpretation encompasses discrimination between men and women but does not encompass discrimination based on gender identity per se, including transgender status. In an extremely interesting case, the Second Circuit in Zarda v. Altitude Express, Inc., Case No. 15-2775, directed briefs to be filed for the following question: “Does Title VII of the Civil Rights Act of 1964 prohibit discrimination on the basis of sexual orientation through its prohibition of discrimination ‘because of . . . sex?’” Id., 2017 U.S. App. LEXIS 13127 (2d Cir. May 25, 2017). The Sessions DOJ filed its amicus curiae brief on July 26, 2017 setting forth the interpretation later codified in Session’s October 4, 2017 memorandum, and specifically rejected the Seventh Circuit Hively decision; alternatively, the EEOC submitted a brief in support of its own guidelines. The Second Circuit heard oral arguments for this issue on September 26, 2017, and the decision is still pending; experts believe the case will provide a stepping stone to the U.S. Supreme Court to finally decide the issue.

State Laws: Twenty states (CA, CO, CT, DE, HI, IA, IL, MA, MD, ME, MN, NJ, NM, NV, NY, OR, RI, UT, VT, and WA), D.C., Guam and PR have statutes that protect against both sexual orientation and gender identity discrimination in employment in the public and private sector. Two (2) states (NH and WI) prohibit discrimination based on sexual orientation only in the public and private sector. Six (6) states (IN, KY, MI, MT, PA and VA) prohibit discrimination against public employees based on sexual orientation and gender identity. Five (5) states (AZ, AK, MO, NC and OH) prohibit discrimination against public employees based on
sexual orientation only; although NC executive order enumerates both sexual orientation and gender identity, but carves out bathroom use prohibition for transgender employees.

**Bathroom Bills** - Legislation or statute that defines access to public facilities, particularly restrooms, by transgender individuals. So far, only North Carolina passed a bathroom bill (HB2) in March 2016, but that bill received a lot of controversy and was partially repealed on March 17, 2017. In addition, there were preliminary injunctions against enforcing HB2 granted by the courts. See, e.g., Carcaño v. McCrory, 203 F. Supp. 3d 615 (M.D. N.C. Aug. 26, 2016) (injunction against University of North Carolina from enforcing HB2). Currently, there are sixteen (16) state bathroom bills pending in 2017 legislation (AL, AR, IL, KS, KY, MI, MO, MT, NY, SC, SD, TN, TX, VA, WA and WY); two (2) states (OK and NJ) have bills pending from the 2016 legislation.

**Education** - As discussed in the Campus Defense Section, there is current litigation pending regarding a school’s obligation to protect transgender students pursuant to the Department of Justice, Department of Education and Office of Civil Rights Title IX directives issued under the Obama Administration and rescinded by the Trump Administration, as well as the nationwide ban on Obama-era directives on the same. See Texas v. U.S., Case No. 7:16-cv-00054-O, 201 F. Supp. 3d 810 (N.D. Tex. Aug. 21, 2016), app. dismissed, 679 Fed. Appx. 320 (5th Cir. Feb. 9, 2017). See also, e.g., G. G. v. Gloucester Co. Sch. Bd., 853 F.3d 729 (4th Cir. April 7, 2017) (vacated preliminary injunction based upon OCR letters relating to transgender bathroom use). Currently, there are fourteen (14) states (CA, CO, IA, IL, MA, ME, MN, NJ, NV, NY, OR, RI, VT and WA) and D.C. that prohibit educational discrimination based on sexual orientation and gender identity; and two (2) states (NM and WI) that prohibit educational discrimination based on sexual orientation only. But see, e.g., Doe v. Boyertown Area Sch. Dist., Case No. 17-1249, 2017 U.S. Dist. LEXIS 137317 (E.D. Pa. Aug. 25, 2017) (denying plaintiffs’ preliminary injunction seeking to prevent school district from permitting transgender individuals from using bathrooms according to gender identity); and Evancho v. Pine-Richland Sch. Dist., Case No. 2:16-01537, 237 F. Supp. 3d 267 (W.D. Pa. Feb. 27, 2017) (granting plaintiffs’ preliminary injunction to prevent school district from: denying bathroom access to transgender students based on gender identity, taking any disciplinary action against transgender students for bathroom use, and refusing to treat plaintiffs consistent with their gender identity in any respect).

**Housing** - The federal Fair Housing Act prohibits housing discrimination based on race, color, national origin, religion, sex, disability, and familial status (i.e., presence of children under the age of 18 in the household or pregnancy), but does not specifically include sexual orientation and gender identity as prohibited bases; however, LGBTQ discrimination is covered if based upon non-conformity with gender stereotypes. See HUD Policy. (note: on October 3, 2017, the DOJ announced its initiative to combat sexual harassment in housing, but only addressed protection of women and did not mention protections specifically of the LGBTQ community (https://www.justice.gov/opa/pr/justice-department-announces-initiative-combat-sexual-harassment-housing). Each state has its
own laws that may apply to private housing discrimination and how it applies to LGBT individuals. Currently, twenty (20) states (CA, CO, CT, DE, HI, IA, IL, MA, MD, ME, MN, NJ, NM, NV, NY, OR, RI, UT, VT, and WA) and D.C. have statutes that protect against both sexual orientation and gender identity discrimination in housing; and two (2) states (NH and WI) that protect against sexual orientation discrimination in housing. Accord, e.g., Romer v. Evans, 517 U.S. 620 (May 20, 1996) (LGBT protections are not “special rights”).

Public Accommodations - As mentioned in the Masterpiece case, supra, the U.S. Supreme Court decision will widely impact this area of the states’ laws, which refer to governmental entities and private businesses (not private clubs with memberships or dues) that provide services to the general public (e.g., restaurants, movie theaters, libraries and shops). Currently, nineteen (19) states (CA, CO, CT, DE, HI, IA, IL, MA, MD, ME, MN, NJ, NM, NV, NY, OR, RI, VT, and WA) and D.C. have statutes that protect against both sexual orientation and gender identity discrimination in public services; and two (2) states (NH and WI) that protect against sexual orientation discrimination in public services.

Adoption - In Campaign v. Miss. Dep’t of Human Servs., 175 F. Supp. 3d 691 (S.D. Miss. Mar. 31, 2016), Judge Daniel P. Jordan III issued a preliminary injunction striking down Mississippi’s ban on same-sex couples from adoption. This decision coupled with the Pavan decision, supra, has effectively made same-sex adoption legal in all fifty (50) states. Embryo adoption is also discussed in the Assisted Reproductive Technology Laws profile.

Future Trends & Opportunities: Things are changing at a rapid pace in the area of LGBT law, as evidenced by recent U.S. Supreme Court decisions and pending decisions in Masterpiece, as well as the outcomes of the military cases, bathroom cases, and employment discrimination cases as outlined above. Currently, Congress is reviewing the Equality Act (#EqualityForward), having been introduced on May 2, 2017, which would amend the Civil Rights Act of 1964 to include protections that ban discrimination on the basis of sexual orientation, gender identity, and sex in the areas of employment, housing, public accommodations, public education, federal funding, credit, and the jury system. If this bill were to pass, then the decisions and worries discussed above would be superfluous.
**ONLINE FANTASY SPORTS LEAGUES & E-SPORTS**

**WHAT IS IT?**

Fantasy sports is an online game that a person joins a league website; assembles virtual teams of actual athletes (including drafts, trades and cuts) while remaining under a salary cap; and earn points based on the actual statistical performance of the players in real-world competitions (i.e., predetermined scoring arrangements) throughout the season; and, the statistics are compiled and compared to see whose fantasy team has done the best. A popular sub-genre is Daily Fantasy Sports (“DFS”), which is an accelerated version where contests last a single day (e.g., baseball or basketball) or two-three days for NFL to get Monday night games. Daily fantasy sports are typically structured in the form of paid competitions (“contest”), and winners receive a share of a pre-determined pot funded by their entry fees; a portion of entry fee payments go to the provider. Fantasy sports are gaining in popularity, with the value of the market predicted to double over the next five years to **reach $5.3 billion by 2021.**

Esports are a form of competition online through video games. The majority of popular esports are team-based games played in leagues or tournaments throughout the year, culminating in one final event. Esports players may compete for money, with prize pools of up to almost $24 billion. The competitive gaming and esports market is **estimated to be worth almost $1.5 billion by 2020.**

Although fantasy sports and e-sports involve online competition, there is **one critical distinction:** whereas players succeed in DFS based on factors that are outside of their control, namely, how well a professional athlete will perform on a given day, the outcome of an esports event is dependent on the player’s knowledge, dexterity, reflexes, and perseverance. Because DFS success is tied, at least in part, to external factors, regulators have been more inclined to classify DFS leagues as “games of chance” that may be regulated (or prohibited) as gambling, whereas e-sports have largely evaded regulatory oversight - though one observer **suggests otherwise.** By contrast, betting on e-sports (as opposed to playing them) is potentially subject to gambling restrictions. [Note: online poker, which is not discussed here, another type of online gaming, is generally regarded as gambling and has been regulated as such. See Wikipedia for summary of state laws on online poker]

**WHY NOW?**

Advances in technology have given participants instantaneous access to information, metrics and data about particular games and players, thereby simplifying the ability to calculate scores from such data and making fantasy gaming more accessible and appealing to a wider audience (approximately 56 million people). Meanwhile, as the prize money for esports tournaments increases, they continue to attract more players.
KEY LEGAL ISSUES APPLICABLE TO FANTASY SPORTS:

Federal Law - The Unlawful Internet Gambling Enforcement Act of 2006 (“UIGEA”) allows fantasy sports, as long as the participants are not betting on the outcome of a particular game or single player’s performance: the prize value is established and clearly communicated in advance and not tied to the number of participants or fees received; and winning should reflect the comparative skill, talent and expertise of the participants. The rationale is that fantasy sports is a game of skill, not of chance. Essentially, the government has left the concern of regulating fantasy sports up to the states. See Legal Sports Report, (9/17/2015)(discussing relationship between UIGEA and state laws, noting that company can comply with UIGEA but still violate state law).

Federal Income Tax Now, the federal government is concerned when it comes to a participant’s winnings; all winnings are considered income that must be reported to the IRS – even if the winnings are not legal in the participant’s jurisdiction.

State Gambling Laws & PAPSA States do have the right to ban specific types of applications, websites and businesses from being legal. Based upon each state’s regulations, fantasy sports leagues are are legally allowed with money exchanged. Five states - Arizona, Iowa, Louisiana, Montana and Washington - ban gambling altogether. Some states have proposed or recently passed laws allowing DFS and in other states, AGs have determined that fantasy sports are a game of skill and thus, is not unlawful gambling.

The Professional Amateur and Protection Act (PAPSA) is a federal law that prohibits states (with the exception of Nevada and Delaware, which are grandfathered) from authorizing “a wagering scheme based on “one or more performances” of athletes in competitive professional or amateur games.” PAPSA therefore prohibits states from legalizing sports gambling. To date, however, states have been able to legalize DFS and bypass PAPSA restrictions by categorizing DFS as something other than a wagering scheme. Moreover, it is possible that the PAPSA restrictions on states’ ability to legalize sports gambling may be eliminated entirely in light of a pending Supreme Court case, Christie v. NCAA (just argued on December 4, 2017) which takes up the question of whether PAPSA unconstitutionally “commandeers” a state’s regulatory power to enforce a federal law.

Employer - Some employers may see allowing or operating a sports fantasy league as fun or a way to boost morale and camaraderie; however, there are legal and practical issues to consider. Allowing a league to operate at the workplace during business hours cuts into employee productivity; according to an Aug. 13, 2014, report by the Heather Draper with the Denver Business Journal, a global employment consulting firm has estimated that employees may waste up to two hours of “on the clock” time per week managing their fantasy teams. If an employer decides to host a league, it should monitor the current status of the jurisdiction’s gambling laws; or operate a league without an entry fee or without rewards or monetary prizes. Additionally, it may be in the
employer’s best interest to have a written policy to protect the business from an employee-operated league for cash, and regularly remind employees of Internet use and gambling policies.

Additional Issues for e-sports: Many esports issues - such as patents, IP and labor issue are more generic in nature and not detailed here. But see Esports Explosion: Legal Challenges & Opportunities, ABA Journal (Nov. - Dec. 2016). However, one interesting issue relates to the question of whether esports players may be classified as athletes. As explained in Forbes (5/17/2017), one of the reasons this debate matters is because if esports gamers aren’t athletes, they don’t qualify for P-1 visas - which means that it can be very difficult for these professionals to travel to the U.S. to participate in major competitive events. See also The Sports Journal 5/11/2017)(making the case for classifying esports gamers as athletes). In the past, e-gamers have been recognized as athletes and granted P-1 visas, but because P-1 visa status is discretionary, past practices are no guarantee of future grants. See e.g., Overwatch Players Denied Visa A Week Before LA Tournament, Esports Observer (10/3/2017).

Future Trends & Opportunities: Currently, the lobbying efforts across the nation have led to favorable opinions and/or legislation supporting fantasy sports. Few states tie the host to a state gaming commission; therefore, there is no government authority that oversees fantasy sports and the scandals involving DraftKings and FanDuel could call for greater government oversight in the industry.

On-Line Fantasy Sports & E-Sports - Update!

On May 14, 2018, the Supreme Court’s ruled in Murphy v. NCAA that PAPSA violated the anti-commandeering principle prohibiting Congress from compelling states to enforce federal law - in this instance, federal laws prohibiting gambling. Finding PAPSA unconstitutional, the Supreme Court vacated the entire statutes. As noted in the main summary, states had found ways to bypass PAPSA with respect to Daily Fantasy Sports (DFS) by characterizing this category of gaming as one of skill rather than wagering. With PAPSA repealed, DFS operators are exploring ways to expand the spectrum of offerings that might also encompass once unlawful wagering. See Bend Bulletin (June 30, 2018).
OPEN SOURCE LAW

WHAT IS IT?
Source code is the original version of software (an application program or an operating system) written in programming language (e.g., C, C++, Java, etc.) through alphanumeric characters (plain text that can be read by a person) and entered into the computer. Open source software (“OSS”), sometimes referred to as collaborative development, is a creative work (such as the human-readable code) made freely available to the public through a license in which the copyright holder expressly provides the rights to study, change, and distribute the software to anyone for any purpose. The legal issues related to open source law are highly technical.

WHY NOW?
Open Source Software is now the backbone of the tech industry, with the rise of substantial investment into open source solutions by IBM, Intel, Facebook, Google, etc. It is impossible to develop software without encountering some form of open-source code either in the platform or as a component. The typical commercial product contains hundreds of high quality open source components, though data shows that only a small percentage of these components are having their open source licensing obligations followed because development practices have outpaced internal corporate process to manage the legal obligations set forth in the licensing requirements; consequently, most companies become out of compliance with legal obligations.

KEY LEGAL ISSUES:

Copyright law - Copyright law as modified by the DMCA 1998 adoption of the Digital Millennium Copyright Act (DMCA), which controls digital rights management (i.e., penalties for copyright infringement on the Internet). The creator of original computer code, including open source is creator of code holds a copyright, but through open source licenses assigns the rights to change, study and alter the software. One problem that arises in dealing with open source and a product built from several pieces of code by different authors is the extent to which each contribution is covered by copyright or open source license. Likewise, failure to adhere to an open source license can be a copyright violation and breaching the license can be subject to punishment.

Work-made-for-hire rule: Copyright belongs to an employer when code is developed by an employee within the scope of his employment (note: an employee should notify company if making a personal open source project and be in compliance with the employee IP agreement and company policy); or belongs to the client that specifically commissioned the production of the code, for any of the enumerated purposes under 17 U.S.C. § 101, pursuant to a written “work-made-for-hire” agreement signed by the developer.
License or Assignment Clause: As negotiated in a development contract, the copyright owner can assign in writing all of the rights in the copyright to another party; or, provide a license to grant permission to use the code without forfeiting ownership.

Open Source platform: Derivative software based on open-source software must generally conform to the terms of the original open source license upon distribution, but software written to perform on an open source platform do not need to conform to the original license (i.e., it is not considered a derivative work).

Types of Licenses: Hailed as the most important OSS case to date and setting legal precedent for the open source movement, Jacobsen v. Katzer, 535 F.3d 1373 (Fed. Cir. 2008) determined that open source license are enforceable under both contract and copyright law. OSS can be licensed under many different licenses, each carrying a different set of requirements for use and/or modification. The most widely used major open source licenses are: Apache 2.0; BSD license; GNU GPLv.3; GNU Library or “Lesser” General Public License (LGPL); MIT License; Mozilla Public License 1.1 (MPL); Common Development and Distribution License; Common Public License 1.0; Eclipse Public License. At time, if the existing license is compatible with a new license, the program can be distributed under the new license. TLDRLegal.com: Software Licenses in Plain English summarizes key terms of dozens of open source licenses.

Trade secrets: A company (or its employee) must determine that the OSS does not include any trade secrets that should not be made available to the general public.

Patents: A company cannot apply for a patent for OSS projects which would constitute public disclosure; or, if project contributions come from patented companies, the contributor will need an express patent grant or CLA (see above); there is the Open Invention Network, a shared defensive patent pool to protect members’ use of major open source projects or explore other alternative patent licensing.

Future Trends & Opportunities:
Most startup companies today not based on, at least in part, on open source; it is not how modern organizations (and some traditional organizations are catching up) build software. Looking ahead, open source legal issues will continue to crop up in the news, possibly with a push to revive patent litigation reform under the Trump Administration.
ORGANIC CERTIFICATION LAW

WHAT IS IT?
In order to advertise an agricultural product as “organic” or to affix a “USDA Organic” label to the product, a seller must certify his product in accordance with the Organic Foods Production Act of 1990 (“OFPA”). Attorneys who practice organic certification law help clients navigate the OFPA’s standards in order to obtain organic certification.

WHY NOW?
Prior to 1990, there was no national standard governing the use of the term “organic.” The OFPA was enacted to create such a standard in order “to assure consumers that organically produced products meet a consistent standard.” Certification under the OFPA has become increasingly valuable as consumers are now willing to pay a premium for organic foods.

KEY LEGAL ISSUES:

False Advertising: One active area of the law concerns the extent to which the OFPA preempts state-law false advertising claims. The leading case on this question is In re Aurora Dairy Corp., 621 F.3d 781 (8th Cir. 2010). In this case, the Eighth Circuit held that the OFPA preempts state-law claims that directly challenge the certification decision—i.e., claims that a USDA certified organic product is not in fact organic. But the court held that the OFPA did not preempt state law challenges that indirectly challenged the certification decision—i.e., by seeking to prove facts showing that the product should not have received organic certification. For example, if a producer of a certified organic product claims that its product does not contain preservatives, that claim may be challenged under state law, notwithstanding the fact that it relies “on proof of facts that, if found by the certification agent, would preclude certification.”

Other courts have disagreed with this analysis, holding that even claims that directly challenge a certification decision are not preempted. See Segedie v. Hain Celestial Grp., Inc., (S.D.N.Y. May 7, 2015). Other courts have considered whether OFPA preempts a state law claim that a producer fraudulently affixed a USDA Organic Label to a product that was not certified (the California Supreme Court held that such a claim was not preempted).

Genetically modified organisms: A related area of law concerns labeling of agricultural products that contain genetically modified organisms (“GMOs”). In 2016, President Obama signed legislation that requires labeling of food products containing GMO ingredients. Producers can use text, a symbol, a phone number to a GMO-information hotline, or a QR code that will direct the consumer to a GMO-information website. Products that contain GMOs are not eligible to receive organic certification, so organic producers will not need to worry about the GMO labeling requirement. But
practitioners of organic certification law may be well positioned to assist with GMO labeling.

**Organic Certification + Cannabis** - USDA organic certification is not available for cannabis because it is a controlled substance - though recently, USDA made an exception and offers organic certification for industrial hemp produced in compliance with applicable state law. See [USDA Regulation re: Hemp, Federal Register, 8/12/2016](https://www.federalregister.gov/documents/2016/08/12/2016-19216/organic-certification-for-industrial-hemp) ; See also [The Cannabist](https://thecannabist.com/2015/09/16/organic-certification-for-industrial-hemp/) (9/16/2015) (describing USDA organic policy). There are, however, private organizations such as [Certified Kind](https://certifiedkind.com) that offer certification for marijuana growers.

**Enforcement issues:** Organic farmers are certified by USDA. Failure to comply with applicable regulations may result in a revocation of certification following a hearing before a USDA administrative law judge.
PERSONAL JURISDICTIONAL ISSUES IN THE AGE OF THE INTERNET

WHAT IS IT?
If you’ve taken civil procedure, you surely recall the infamous Int’l Shoe Co. v. Washington, 326 U.S. 310 (1945) opinion and the concept of personal jurisdiction, i.e. the requirement that a given court have power over the defendants based either on some nexus to the chosen forum. Traditionally, personal jurisdiction has been established through (1) physical presence through residence or business (in personam), (2) ownership of property (in rem), (3) choice of law contract provisions or (4) a minimum contacts test typically codified in state long arm statutes that allows jurisdiction to attach either through “continuous and systematic” contact with the forum unrelated to the cause of action (general jurisdiction) or direct contact related to the cause of action (specific jurisdiction). Notice of a lawsuit is also necessary to establish personal jurisdiction over a defendant.

WHY NOW?
In an Internet Age, defendants are everywhere but also nowhere. For example, does a blogger in New Jersey penning defamatory articles about a restaurant in California for a blog with national reach have sufficient contacts in California to trigger personal jurisdiction if sued there? What about a mom selling baby toys online all over the country from her home in Kentucky, taking out Facebook ads to target East Coast customers? If the toy injures a child and her parents file suit in Maine, can the mom be hauled into the court? Service requirements are changing as well, with many folks - particularly Gen X and Millennials - more likely to open up a message on Facebook or text than to pick up a certified letter at the post office containing a summons. The issue that lawyers must ask is whether these technology changes also change the requirements of personal jurisdiction?

KEY LEGAL ISSUES:

Personal Jurisdiction: In Walden v. Fiore, 134 S. Ct. 1115, 1125 n.9 (2014), the Supreme Court explicitly left “questions about virtual contacts for another day” and did not address minimum contacts where intentional torts are committed via the Internet or other electronic means. As a result, much of the applicable caselaw has been developing through lower courts, with limited uniformity between rulings on personal jurisdiction. Below are three primary tests applied by courts in evaluating whether and to what extent internet contacts may give rise to personal jurisdiction.

Zippo test: The most widely adopted analysis is derived from Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997), having been cited more than 5,000 times. The Zippo court set forth a “sliding scale” of internet activity to determine if a site was “passive” (i.e., static content), “interactive,” or “commercial” to avail
itself to certain state’s laws; holding, a passive webpage is insufficient to establish personal jurisdiction, but an interactive site through which a defendant conducts business with forum residents is sufficient. The Third Circuit in Toys “R” Us, Inc. v. Step Two, S.A., 318 F.3d 446 (3rd Cir. 2003) approved of the Zippo test. Since the Zippo test was adopted, however, the internet has evolved significantly from website disputes to the wide use of social media. Recently, in Sioux Transportation v. XPO Logistic, Case No. 5:15-CV-05265, 2015 U.S. Dist. LEXIS 171801 (W.D. Ark. 2015), the court opined:

[T]he Court had the “difficulty in considering the Zippo test in the context of the modern internet. The internet has undergone tremendous change since Zippo was decided in 1997, and even since [Johnson v. Arden, 614 F.3d 785 (8th Cir. 2010)]. Cloud computing has eliminated the need for downloading files in many situations, location-based technology has made online interactions that formerly existed only in cyberspace more closely tied to specific geographic locations, and the level of user interaction with websites has exploded with social media. All of this calls into question the modern usefulness of the Zippo test’s simplistic tri-part framework: The transmission of computer files over the internet is perhaps no longer an accurate measurement of a website’s contact to a forum state.

See also Atlasware, LLC v. SSA, Case No. 5:16-cv-05063, 2016 U.S. Dist. LEXIS 87991 (W.D. Ark. 2016) (“this Court recognizes that ongoing technological advances affecting how such information is stored and accessed require courts to continuously fine-tune the process for making that [jurisdictional] evaluation.”).

Moreover, many courts have opined that the Zippo test is limited in its application to specific jurisdiction and not general jurisdiction issues; appellate courts are split in its applicability to the latter. See, gen., Gator.com Corp. v. L.L. Bean, Inc., 341 F.3d 1072 (9th Cir. 2003) (applying Zippo and finding general jurisdiction); Gorman v. Ameritrade Holding Corp., 293 F.3d 506 (D.C. Cir. 2002) (same); Soma Med. Int’l v. Std. Chtd. Bank, 196 F.3d 1292 (10th Cir. 1999) (same). Compare Revell v. Lidov, 317 F.3d 467 (5th Cir. 2002) (holding Zippo is not well adapted to the general jurisdiction inquiry); and Bell v. Imperial Palace Hotel/Casino, Inc., 200 F. Supp. 2d 1082 (E.D. Mo. 2001) (combining Zippo with other factors).

Calder test: The effects test identified in the aforementioned Calder case and routinely applied in torts cases, results in personal jurisdiction if the harm occurs in the forum state and defendant knew it would occur there. See, e.g., Young, supra; Healthgrades.com Inc., supra; Yahoo! Inc. v. La Ligue Contre Le Racisme et l’antisemitisme, 433 F.3d 1199 (9th Cir. 2006) (en banc); Blakey v. Cont’l Airlines, 751 A.2d 538 (N.J. 2000); Schwarzenegger v. Fred Martin Motor Co., 374 F.3d 797 (9th Cir. 2004) (no jurisdiction where the audience was Ohio rather than California); Dudnikov v. Chalk & Vermilion, 514 F.3d 1063 (10th Cir. 2008); and Boschetto v. Hansing, 539 F.3d 1011 (9th Cir. 2008); Tamburo v. Dworkin, 601 F.3d 693 (7th Cir. 2010); and Baldwin v. Fischer-Smith, 315 S.W.3d 389 (Mo. Ct. App. 2010). The Calder test, however, is limited to inquiries of specific jurisdiction (See, e.g., Carefirst of Maryland, Inc. v. Carefirst Pregnancy Centers, Inc., 334 F.3d 390, 398 n.7 (4th Cir. 2003) (categorizing Calder as the “effects test of specific jurisdiction”), and is not helpful to general jurisdiction questions.
Mohasco test: In internet-based cases, the Sixth Circuit has employed a three-part test developed pursuant to S Mach. Co. v. Mohasco Indus., Inc., 401 F2d 374 (6th Cir. 1968) to determine personal jurisdiction: (1) the defendant must purposefully avail himself of the privilege of acting in the forum state or causing a consequence in the forum state; (2) the cause of action must arise from the defendant's activities there; and (3) the acts of the defendant or consequences caused by the defendant must have a substantial enough connection with the forum state to make the exercise of jurisdiction over the defendant reasonable. See, e.g., Bird v. Parsons, 289 F3d 865 (6th Cir. 2002); Neogen Corp v. Neo Gen Screening, Inc., 282 F3d 883 (6th Cir. 2002); Columbia Pictures Indus., Inc. v. Fysh, Case No 5:06-CV-37, 2007 U.S. Dist. LEXIS 11234 (W.D. Mich. 2007); Dedvukaj v. Maloney, 447 F. Supp. 2d 813 447 F. Supp. 2d 813 (E.D. Mich. 2006); and Hinners v. Robey, No. 2009-SC-000389-DG, 336 S.W.3d 891 (Ky. 2011).

Service of Process: Under the constructive notice principles, is an emerging class of substitute service to effectuate jurisdiction, is service by e-mail and by social media accounts, such as Twitter and Facebook.

Service by email - A few courts have allowed service by email primarily as an alternative when service could not be effected in a traditional manner. See e.g., S. Commodity Futures Trading Com’n v. Rubio, 2012 WL 3614360 (S.D.Fla., August 21, 2012)(granting leave to plaintiffs to serve by email when defendant cannot otherwise be located); Snyder v. Energy Inc., 857 N.Y.S.2d 442 (2008), (allowing service of process through e-mail where corporation not registered with the state). See also WhosHere, Inc. v. Orun, 2014 U.S. Dist. LEXIS 22084 (E.D. Va. 2014 acknowledging “[s]everal courts have permitted service of process by email and other electronic communications” (citing cases));

Service via social media. Courts have acknowledged that service by Facebook is a relatively “novel concept,” and “that it is conceivable that defendants will not in fact receive notice by this means;” however, courts must remain open to “considering requests to authorize service via technological means of then-recent vintage.” F.T.C. v. PCCare247 Inc., 2013 U.S. Dist. LEXIS 31969, 2013 WL 841037, at *5 (S.D.N.Y. 2013) (citing cases and holding that service by both email and Facebook satisfies the due process inquiry). Service by Facebook, however, has only been allowed in cases where “the proposed service by Facebook is intended not as the sole method of service, but instead to backstop the service upon each defendant at . . . its[ ] known email address.” Id.; but see Fortunato v. Chase Bank USA, 2012 U.S. Dist. LEXIS 80594, 2012 WL 2086950, at *2 (“Service by Facebook is unorthodox to say the least” and plaintiff had not set forth “any facts that would give the Court a degree of certainty that the Facebook profile . . . is in fact maintained by [defendant] or that the email address listed on the Facebook profile is operational and accessed by [defendant]”). See also, e.g., D.R.I., Inc. v. Dennis, 2004 U.S. Dist. LEXIS 22541 (S.D.N.Y. 2004); Lipenga v. Kambalame, 2015 U.S. Dist. LEXIS 172778 (D. Md. 2015) (“Service through these channels comports with due process because it is reasonably calculated to provide Defendant notice of this suit”); Facebook, Inc. v. Banana Ads, LLC, 2012 U.S. Dist. LEXIS 42160 (N.D. Ca. 2012). Accord, Ferrarese v. Shaw, 164 F. Supp. 3d 361 (E.D.N.Y. 2016) (court permitted service of process via email and Facebook account, but plaintiff was required to send a copy via
Future Trends & Opportunities: Based upon the Supreme Court’s statement in Walden, it will likely address the jurisdictional questions arising in Internet cases in the near future. In the meantime, the lower courts will continue to move away from the Zippo test and adopt more effective means of determining personal jurisdiction in Internet-related contacts as more and more cases arise out of social media communication and publication. In addition, service of process by email or social media will continue to be included as a viable alternative means just like any type of publication. The legal community has always evolved with technology, and included that evolution into its decisions and legislation to permit society to easily access the court system.
PRIVACY LAW ONLINE

WHAT IS IT?

Privacy law refers to the laws that deal with regulating, storing, and using of personally identifiable information of individuals, which can be collected by governments, public or private organizations, or by other individuals. See generally, Wikipedia. Generally, privacy law focuses on issues such as (1) whether a user gave informed consent to data collection and (2) what harm results when personally identifiable information (PII) is compromised through hacking, misappropriation or undisclosed use? Both federal and state law (as well as ethics rules for lawyers) establish standards governing entities that collect information. Companies doing business overseas must also comply with other countries privacy laws - for example, the European Union’s Data Privacy laws, which are particularly stringent. (Note - discussion of EU Data Privacy Law and other international standards is beyond the scope of this section)

WHY NOW?

Although information privacy has always been a concern, in a paper world, data could survive for decades in practical obscurity, inaccessible even to those who collected it. In an interconnected, online world, personal information is more vulnerable to hacking, with grievous consequences, such as identity theft or stolen financial information. Today’s technology also encourages collection of data through websites because the tools are now available to analyze and glean business insights from this “big data.” Moreover, data collection is no longer limited to addresses and zip codes: with the Internet of Things (See Section on IoT), companies can gather information on energy use, hours spent working out or even personal sexual habits. Not only is this data more personal and potentially invasive, but as data analytics increase in sophistication, much of this information can easily be de-anonymized. See also Biometric Identification (discussing privacy and other issues unique to biometrics).

KEY LEGAL ISSUES:

In the United States, there are a myriad of federal and state laws and regulations that govern collection, storage and use of personal information, along with obligations in the event of breach. (See Cybersecurity Section for discussion of data breach obligations).
**Standing:** Spokeo v. Robins, 136 S.Ct. 1540 (2016) held that a plaintiff alleging a violation of a privacy statute lacks standing to sue absent a showing of particularized, concrete harm, and remanded the case to the Ninth Circuit. On remand, the Ninth Circuit found standing, writing that "It does not take much imagination to understand how inaccurate reports [showing inaccurately that Robins was employed, had children and was wealthy] on such a broad range of material facts about Robins’ life could be deemed a real harm.” See Spokeo, 867 F.3d 1108 (9th Cir. 2017), cert petition filed, (December 4, 2017). See also Clapper v. Amnesty Intern, 133 U.S. 1138 (2013), (rejecting challenge surveillance under FISA, finding that fears of hypothetical future harm do not satisfy Article III).

Together, Spokeo and Clapper pose a hurdle to plaintiffs bringing suit in hopes of changing data collection practices, or for fear of future harm - as in data breach cases, where harm is not immediately known. Establishing standing is even more challenging given the conflicting cases that emerged in the wake of Spokeo. In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 274 (3d Cir. 2016), cert. denied sub nom. C. A. F. v. Viacom Inc. (U.S. Jan. 9, 2017) (alleged disclosure of information about personal online behavior in violation of state and federal privacy statutes is concrete and particularized injury-in-fact), Brian Mount v. PulsePoint (2nd Cir 2017) (finding standing because alleged circumvention of web-browser privacy features and its placement of tracking cookies on plaintiffs’ computers in order to gather information about their internet use violates privacy, but finding no cognizable injury); Attias v. Carefirst, 865 F.3d 620 (D.C. Cir. 2017) (finding standing to sue company for data breach resulting in release of PII like credit card and SS numbers which put Ps as serious risk for financial fraud); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) (finding fear of future identity theft insufficient to establish a non-speculative, imminent injury-in-fact for purposes of Article III standing), , 846 F.3d 625 (3rd Ci 2017)"Even without evidence that the Plaintiffs' information was in fact used improperly, the alleged disclosure of [their] personal information created a de facto injury.” gives rise to claim under Fair Credit Reporting Act).

**Personally Identifiable Information (PII)** Personally identifiable information or PII is generally understood to mean is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. See generally Wikipedia (PII definition). But the question of what constitutes collection of PII is not necessarily straightforward - because with today’s technology tools, a company may be able to figure out a user’s PII based on seemingly anonymized data. Several recent cases under the Video Privacy Protection Act (VPPA) - which bars disclosure of users’ PII - address this question. In Eichenberger v. ESPN, Inc., No. 15-35449, 2017 WL 5762817 (9th Cir. Nov. 29, 2017), the user alleged that ESPN violated the VPPA by sending the serial number of his Roku device with other viewing data to
Adobe Analytics which could match that data with information from other sources to identify the user personally. The Ninth Circuit rejected the claims, finding that that Congress had intended PII (as the term is used in the VPPA) to include only information that “readily permit[s] an ordinary person to identify a specific individual’s video-watching behavior” and that a Roku serial number alone would not allow a lay person to figure out the user’s viewing patterns. See In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 284 (3rd Cir. 2016)(adopting ordinary person standard in VPPA case to find that IP address alone incapable of identifying PII); but see Yershov v. Gannett Satellite Info, 820 F.3d 482, 486 (1st Cir. 2016)(holding that the term "personally identifiable information" encompasses "information reasonably and foreseeably likely to reveal which . . . videos [a person] has obtained).

**Data Collection:** Although collecting consumer data is not per se unlawful, doing so without disclosure and consent may violate state or federal law. The FTC treats failure to disclose data collection as a deceptive practice and has brought enforcement actions against companies that collected customer information without disclosure. See FTC-Vizio Settlement (2/2017)(enforcement action against Smart TV company for identifying and collecting viewing data, selling viewing histories to ad companies and providing consumer IP addresses to data aggregators to target ad campaigns); FTC-Upromise (3/2017)(action against company for failure to clearly and prominently disclose the collection and use of consumer data by its RewardU toolbar). There have also been a myriad of lawsuits alleging privacy violations for undisclosed data collection. See Casper-Navistone Lawsuit, Digital Trends (12/2017)(lawsuit against mattress company by consumer alleging sale of information collected from browsing site to a 3rd party that was able to determine his PII); Bose Headphones Lawsuit, Chicago Tribune (12/2017)(alleging violation of federal Wiretap Act and Illinois eavesdropping and consumer fraud laws by tracking user listening habits and sharing without consent); UnrollMe Hit With Privacy Suit of Alleged Sale of User Data, CNET (4/27/2017)(suing free service that promises to organize inbox by sorting subscription email, then tracking emailed Lyft receipts and selling them to Uber, without disclosing data sales as part of terms of service); see also Section on IoT re: privacy).

**Other Privacy Statutes** - In addition to the statutes discussed supra, there are others - many industry-specific - governing collection of PII and breach notification procedures specific to certain industries. See e.g., Cybersecurity re: Breach Notification. the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §1301 and Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule) (45 C.F.R. Parts 160 and 164); The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827)(applicable to collection, use and disclosure of financial information, applicable to banks, securities firms and others that provide financial services) a Electronic Communications Privacy

**Future Trends & Opportunities:** Privacy law will continue to be a significant issue over the next decade with the emergence of new technologies - IoT, self-driving vehicles, chatbots and more that collect information, along with more sophisticated tools to potentially de-anonymize data. In addition, these technological advances may eventually facilitate the task of establishing standing. Laws and practices governing disclosure will evolve (for example, do click wrap terms of service offer sufficiently meaningful disclosure to inform consent), and lawyers will be called upon by both consumers and companies to test - or even re-calibrate the balance between privacy and consumer demand for convenience. Privacy still remains a lucrative field with multiple opportunities to represent established companies and startups on compliance, and consumers raising invasion of privacy claims.

Equally important, most states either have general security laws or laws that require specific safeguards generating the obligation for lawyers to develop and maintain “reasonable measures” to protect categories of personal information (they vary among states but the categories defined by the FTC and enumerated above are the ones usually retained by states too).
ROOFTOP SOLAR LAW

WHAT IS IT?
In recent years, businesses and homeowners have begun installing solar panels on their rooftops in order to generate emission-free electricity. Rooftop solar law encompasses all of the legal questions related to installation and operation of these panels.

WHY NOW?
Falling costs, combined with federal, state, and local incentives, have lead to explosive growth in rooftop solar. By one estimate, rooftop solar installations have increased by as much as 900 percent over the past six years. The residential solar-financing industry has grown from a $1.3 billion dollar industry in 2012 to a $5.7 billion industry in 2016.

KEY LEGAL ISSUES:
Restrictions on ability to install solar panels: Although many cities have adopted solar-friendly zoning regulations, other cities may limit where solar panels can be installed, or require homeowners to seek special use permits to install panels. Homeowners associations may also attempt to prevent a homeowner from installing solar panels. In some cases, historic preservation laws may require a homeowner to seek permission before making modifications to her home. If a local government or HOA seeks to prevent the homeowner from installing solar panels, the homeowner should check to see if her state has adopted a solar access law. These laws either preempt local ordinances that restrict rooftop solar, prohibit private entities from enforcing contracts or covenants that prohibit rooftop solar, or both.

Solar Easements - If there are no legal barriers to installing a solar panel, the homeowner should determine whether there are any physical barriers to the effective operation of her panels. If the homeowner is concerned that vegetation or structures on a neighboring property may someday block her access to the sun, she may want to consider obtaining a solar easement from her neighbor.

Selling excess power - A related question is whether the homeowner will be allowed to sell excess power back to the grid at retail price—a practice known as “net metering.” The utility industry has been vigorously lobbying against net metering, with considerable success. See Rooftop Solar Dims Under Pressure from Utility Lobbyists, N.Y. Times (Oct. 5, 2017) However, selling excess power is still an option in some states, and offers an additional opportunity to defray costs.

Consumer Protection Issues - As competition in the solar industry grows, so too do more aggressive tactics to lure customers. In 2016, the Federal Trade Commission held a workshop on consumer protection issues - such as false claims regarding cost of panels. See FTC Workshop Transcript. As of 2017, the FTC had received

**Future Trends & Opportunities:**
While many states and municipalities are erecting barriers to rooftop solar, some are actually moving forward with solar mandates. California law requires all new buildings that have 10 or fewer floors to designate 15 percent of the rooftop as “solar ready.” Earlier this year, San Francisco became the first major city in the United States to require builders to actually install solar panels on these buildings. The mandate is expected to provide about 10.5 gigawatt hours of electricity annually, enough to power 2,500 homes. The City of South Miami recently enacted its own solar mandate.
SHARING ECONOMY (AKA “GIG” ECONOMY’)

WHAT IS IT?
The term “sharing economy” is an umbrella term that encompasses platforms that use internet, smartphone, and software technologies to create marketplaces that facilitate on-demand transactions between numerous peers – decentralized buyers and sellers who are frequently individuals or small entities. Sharing economy platforms enable “the emergence of marketplaces, . . . meeting point[s] for supply and demand, making it easier for almost anyone to become a supplier of goods and services in exchange for money.” See FTC Report on Sharing Economy (2016). AirBnB - where home or apartment owners can rent space to The “gig economy” refers to a distinct subset of the sharing economy, specifically, the delivery of services like transportation (Uber or Lyft) household tasks (TaskRabbit) or freelance legal services (PrioriLegal, Hire an Esquire).

WHY NOW?
Several factors account for the rise of the sharing economy. Technology enabled the creation of platforms where providers can offer goods and services efficiently. Moreover, launching on the heels of the recession, corporate downsizing and increased student loan debt, sharing economy sites quickly gained traction because they offered a second revenue stream to the underemployed and lower-cost and more convenient services to busy and budget-minded consumers. PricewaterhouseCoopers estimated that five key sharing economy sectors generated $15 billion in revenues worldwide in 2013, predicted to increase to $335 billion by 2025. See http://pwc.blogs.com/press_room/2014/08/five-key-sharing-economy-sectors-could-generate-9-billion-of-uk-revenues-by-2025.html.

KEY LEGAL ISSUES:
Because many sharing economy businesses disrupt existing incumbent businesses, they often evade the same regulation that govern traditional providers. The regulatory gap creates uncertainty which, despite many lawsuits still persists either because mandatory arbitrary clauses in user agreements has blocked litigation, or the platform settled quickly to avoid risk of future liability. As such, applicable law continues to evolve.

Privacy - Sharing economy platforms often collect personal user information and retain credit card information for billing. Other platforms like Uber track users’ location even long after the ride has completed - a controversial practice that Uber ended in August 2017. See NPR Report (8/29/2017). Also in August 2017, Uber agreed to implement a comprehensive privacy program and obtain
regular, independent audits to settle Federal Trade Commission charges that the ride-sharing company deceived consumers by failing to monitor employee access to consumer personal information and by failing to reasonably secure sensitive consumer data stored in the cloud. See FTC Press Release (8/2017)

**Discrimination and Civil Rights Violations**: Because sharing economy platforms merely facilitate transactions between individuals (who are generally not subject to discrimination laws), these sites raise questions about whether and to what extent discrimination laws apply to the platform itself. The issue of race-based discrimination takes on heightened significance as consumers become increasingly reliant on sites like Uber or AirBNB, and in light of new evidence of bias. See, e.g., Uber & Lyft and False Promises of Fair Ridership, Atlantic, (describing studies showing black Uber and Lyft passengers face longer wait times and greater chance of cancellation); Courthouse News (11/15/2017) (noting that iBnB offers black renters 16 percent fewer places to stay than white); Discrimination Evidence from TaskRabbit, online at Dataworkshop.

To date, the extent of a platform’s liability for race discrimination against users remains unsettled due to procedural hurdles in reaching the merits. See Selden v. Airbnb, 1:16-cv-0093 (2016)(race discrimination class action precluded by Airbnb’s terms of service requiring arbitration of claims, and dismissing suit); See Harrington v. Airbnb, Case 3:17-cv-00558 (D. Oregon July 2017)(pending motion to dismiss race discrimination class action for want of standing based on allegations that lead plaintiff never used AirBNB). By contrast, individual hosts are subject to liability for discrimination in California. See Air BnB Discrimination, LA Times, 7/13/2017. (California fair housing regulators levied a $5000 fine against an AirBNB host who used a racial slur when backing out of a rental agreement with an Asian woman).

Sharing platforms have been more proactive in attempting to ensure access for disabled passengers, presumably in an effort to avoid liability, with mixed results. AirBNB bought Accomoble in November 2017, a niche site focused on disabled-friendly accommodations and began asking hosts to provide more detailed information on accessibility in postings. See Air BnB Buys Acommable, Tech Crunch (11/16/2017). But Uber’s efforts to improve options for the disabled with the introduction of WAV (wheelchair accessible vehicle) service fell short: too few drivers offered WAV service resulting in waits of up to 45 minutes by disabled passengers and Uber charged added fees for WAV service. Even after its WAV initiative, Uber now faces at least two discrimination lawsuits in New York and Washington D.C. involving disabled travelers. See Uber Disabilities Lawsuits in NYC, NYT, 7/18/2017. (New York suit), Uber Sued for Disabilities Violations in DC, CNN (6/8/2017)(D.C. suit alleging violations of Americans with Disabilities Act and D.C. Human Rights law).

**Zoning and Housing Laws**: Some jurisdictions or building owners have laws that prohibit short term apartment rentals or operation of unlawful hotels that prohibit owners from leasing rooms on AirBNB. New York City has been particularly aggressive in enforcing its laws prohibiting short-term rentals; most recently, officials sued two landlords for violations and settling the matter for $1 million. See Landlords Reach Illegal Settlement, NY Daily News (11/30/2017). A Los Angeles management company sued AirBNB for providing a platform that enables tenants to violate building regulations that
Independent Contractor Status: A Forbes columnist recently observed that the resolution of whether Uber drivers are employees will “shape the sharing economy.” See https://www.forbes.com/sites/omribenshahar/2017/11/15/are-uber-drivers-employees-the-answer-will-shape-the-sharing-economy/#1e89d48b5e55. The test for whether a worker is a contractor or employee is fairly well-settled, examining factors such as hiring party’s degree of control and supervision, whether providers use their own tools to provide the service and whether the service relates to the hiring company’s core business. See e.g., Borello & Sons v. Department of Industrial Relations, 8 Cal. 3d. 341 (1989). Yet courts and arbitrators have arrived at conflicting decisions when applying these factors. See YE v. Uber Technologies, (2016), online at http://pdfserver.amlaw.com/ca/uber_petition.pdf (arbitrator finds Uber driver is independent contractor) and McGillis v. Florida Dept. of Empl. Opportunity finding Uber drivers not employees entitled to unemployment compensation) but see rulings by California and New York Labor Commission (classifying Uber drivers as employees).

Tort Liability: Under traditional employment law principles, employers are potentially liable for tortious acts by employees acting within the scope of employment under the doctrine of respondeat superior (essentially, vicarious liability) or due to negligent hiring and supervision. But do these same principles apply to sharing economy platforms? It’s a critical question, because most platforms stress that they are technology companies that merely connect individuals with third-party drivers, and not employers or service providers themselves. This characterization allows companies to evade liability for accidents through broad terms of service (TOS) clauses that
absolve these sites of harm resulting from the transaction between a user and a service provider. See Mark Macmurdo, Hold the Phone - Peer-to-Peer Ridesharing Services, Regulation, and Liability, 76 La. L. Rev. (2015).

Recent cases suggest that courts are not inclined to summarily let Uber off the hook for intentional torts by drivers, notwithstanding defenses based on TOS or the undefined nature of drivers' employment status. See e.g., Search v. Uber Technologies, Inc., No. 15-257, (D.D.C. 2015)(allowing respondeat superior claims against Uber by passenger assaulted by knife-wielding driver to proceed because “a reasonable factfinder could conclude that Uber exercised control over [its driver here] in a manner evincing an employer-employee relationship”); Doe v. Uber Technologies, 184 F. Supp. 3d 774 (ND Ca. 2016)(denying motion to dismiss Uber suit involving driver’s sexual assault against passenger because (1) California law does not bar vicarious liability against company for intentional acts if foreseeable and (2) sufficient facts regarding negligent hiring practices and background checks - case since settled).

Another question related to ride sharing platforms is whether they are common carriers - which would subject them to additional regulatory oversight and more stringent safety standards. In Doe v. Uber, supra, the court also found that sufficient facts were alleged to warrant classification of Uber as a “common carrier” subject to a heightened standard of care. A recent class action on behalf of two women sexually assaulted by Uber drivers (Doe v. Uber Technologies, 3:17-cv-06571 (N.D.Ca. Nov.November 2017)) alleges that Uber’s continued classification of itself as a technology platform and a transportation company enabled it to evade the more stringent background check requirements and full disclosure of past assaults.

Insurance Coverage: Insurance practices by sharing economy providers vary. Many states (e.g., California, Florida and Pennsylvania) require transportation providers to have insurance coverage - though these state laws merely codify existing practice, since many established sharing platforms (Uber, AirBNB, TaskRabbit) now carry insurance for harm suffered by customers, subject to different limits and exclusions - e.g., intentional tort. Still, this coverage may not be sufficient so providers must still determine whether their individual homeowners or driving insurance would cover the gap. See e.g., https://www.nytimes.com/2014/12/06/your-money/airbnb-offers-homeowner-liability-coverage-but-hosts-still-have-risks.html?_r=0).

Future Trends & Opportunities:
As the above-discussion shows, much of the law applicable to the sharing economy is still evolving - and therefore, presents unique opportunities for lawyers to make new precedent, either through the judicial process or legislative action.
BONUS #1: Special Ethics Considerations for Freelance Lawyers Serving Other Lawyers:

Increasingly, lawyers are able to avail themselves of the gig economy’s benefits through sites like Hire An Esquire or independent freelance lawyers like Lisa Solomon, QuestionofLaw.net. In using these services, the following ethics considerations apply:

Unauthorized Practice of Law: Can a firm hire a freelancer to research legal matters in jurisdictions where the freelancer is not licensed? Most allow this, so long as the freelancers do not appear before a court where they are unlicensed and are supervised by an admitted attorney. See e.g., Winterrowd v. Am. Gen’l Annuity Ins., 556 F.3d 815 (9th Cir. 2009) (finding that Oregon attorney assisting attorney in litigation in California did not commit UPL since he was supervised by the primary attorney and did not sign pleadings).

Fees & Fee Splitting: The ABA does not consider a markup on contract lawyer fees to be fee-splitting. Instead, ABA Formal Ethics Opinion 2000-420 provides that “When costs associated with legal services of a contract lawyer are billed to the client as fees for legal services, the amount that may be charged for such services is governed by the requirement of ABA Model Rule 1.5 that a lawyer’s fee shall be reasonable.” Most jurisdictions, except for Maryland and Texas have adopted the ABA’s position. See Where Should Firms Draw the Line on Contract Lawyers, online at law.com (2017); Many jurisdictions do not require disclosure of the markup (e.g., California); although others do (e.g., New York) (see http://www.newyorklegalethics.com/dividing-a-fee-with-a-per-diem-lawyer/) Still other states - such as Arizona - define a legal fee as a “fee paid by a lawyer to a client” - and therefore, fees paid by a lawyer to a contract lawyer fall outside the scope of fee splitting.

Duty of Supervision: Under ABA Opinion 88-356, a firm is not obligated to inform the client about using contract attorneys on a matter, as long as those attorneys work under the close supervision of the hiring firm. Moreover, lawyers have always had a duty to supervise less experienced lawyers, and this duty does not changed when the junior lawyer is a freelancer rather than a new associate.

Confidentiality and Conflicts: Ethics on confidentiality and conflicts of interest continue to apply to contract lawyers just as they would to lawyers within a firm.
Sites like Upcounsel.com, PrioriLegal.com and LegalReach.com are platforms that enable small businesses to hire lawyers for specific needs. Companies post projects (e.g., incorporation, patent application, contract review), and solicit proposals for handling the work from lawyers registered with the site. Once clients accept a proposal, the attorney performs the work and on completion, invoices the client through the platform, which remits payment to the lawyer and retains a percentage for administrative and marketing fees associated with the operation of the platform. This model - common to all legal services sharing platforms - implicates concerns about fee-splitting because the client’s payment for services is "split" between the attorney and the platform, which is a non-attorney (as described above, these concerns don’t come into play for freelance contracts because most jurisdictions do not consider the cost that lawyers pay for contract labor to be a "fee."). Several jurisdictions have determined that services offered by attorneys through Avvo (customers pay a flat fee for a lawyer to answer questions or handle a matter like a divorce or will, Avvo holds the payment until the work is complete then remits it to the lawyer, while retaining a percentage) violate fee-splitting rules but have offered some guidance on a compliant path forward. See Virginia Bar Takes Aim at Avvo, online at Lawyerist (6/2017). Lawyer who choose to offer services through third party platforms should familiarize themselves with their jurisdiction’s position on the ethics of sharing platforms that facilitate transactions between lawyers and the ultimate client - or the lawyers themselves may face disciplinary action.
SOCIAL ENTREPRENEURSHIP

WHAT IS IT?

Simply put, social entrepreneurship involves the use of traditional entrepreneurial principles to address society’s problems. See What is a Social Entrepreneur?, ASHOKA, [https://perma.cc/JR84-5BCG]. Social entrepreneurs are driven by a distinct profit motive (unlike most non-profits) but they are also willing to sacrifice earnings (unlike a corporation) to advance their social mission. Social entrepreneurship is also characterized by innovation - leveraging technology tools like crowdfunding, online marketplaces as well as new business models to solve longstanding social problems like poverty, violence against women and inequality.

Social entrepreneurship takes many forms. There’s the “buy one, give one model” employed by Warby Parker, an eyeglass company that aims to solve the problem of helping the 2.5 billion people globally who need glasses but don’t have them by giving away a pair for each pair bought, and TOMS, which a shoe which donates a pair of shoes to a needy individual for each pair sold. Other models include social impact crowdfunding like Kiva, which offers tiny micro-loans as low as $25 to individual, low-income entrepreneurs around the world. Though organized as a non-profit, Kiva fits within the social entrepreneurship category because it is using business tools like loans to solve the problem of poverty. Finally, there’s the “social value enterprise” (SVE) exemplified by the California Fruit Wine Company that adheres to three principles: using profits (beyond those reinvested in the company) to fund startup loans to other SVEs, democratic ownership and remaining in employees’ hands (i.e., never being sold).

WHY NOW?

Social enterprises are an ideal fit for millennials now entering and gaining influence in the business world. Millennials long rejected many of the conventional precepts of the corporate world, and instead, have demanded work-life balance and the opportunity to do well and do good. Other factors accounting for the rise of social enterprise includes technology which reduces start-up costs, the emergence of new corporate structures like the public benefits and L3L corporations which give companies more options and the increased availability of resources in colleges, graduate schools and online to educate those interested in starting social enterprises.

KEY LEGAL ISSUES:

Corporate Formation Issues: One of the most significant issues faced by social enterprises is choice of corporate structure - since that decision will impact the company’s business strategy, governance, scope of fiduciary duty to shareholders, funding options and taxes. There are many possible structures for social enterprise which include: (1) the traditional nonprofit structure which typically
involves formation of a nonstock corporation or LLC and application to the IRS for approval as a 501(c)(3); (2) the benefits corporation, a type of corporate structure available in 30 states and which have an expanded social or public benefit purpose beyond maximizing share value and are required to consider/balance the impact of their decisions not only on shareholders but also on their stakeholders; (3) the benefits LLC, available in Maryland and Oregon (same concept as benefits corporation but applied to LLC); (4) the L3C, an entity created to bridge the gap between nonprofit and for-profit investment by providing a structure that facilitates investment in social enterprises and (5) the B-corporation, which are for-profit companies certified by the nonprofit B Lab to meet rigorous standards of social and environmental performance, accountability, and transparency. See Bcorporation.net; see also http://clsbluesky.law.columbia.edu/2016/08/22/gibson-dunn-identifies-a-corporate-paradigm-shift-public-benefit-corporations/ (summarizing pros and cons of benefits corporations) and Guide To Going B, online at https://cbey.yale.edu/programs-research/an-entrepreneur%E2%80%99s-guide-to-going-b

Fiduciary Duty - As described above, benefits corporations and LLCs must consider not just the interests of shareholders, but also other stakeholders. Although lawsuits for breach of fiduciary duty against directors and officers of conventional corporation abound, because benefits corporations are a relatively new development, litigation history on this topic is limited. See https://wsandco.com/do-notebook/b-corp/

Estate Planning - A recent law review article introduced a new set of legal issues unique to social enterprise: estate planning. See K. Stratton, Making Millennial Money Matter: Benefit Corporations and Their Role in Estate Planning for Social Entrepreneurs, (Keven Stratton), 8 Est. Plan. & Cmty. Prop. L.J. (2016). Stretton writes “[Social entrepreneurs] will have dedicated their careers to making the world a better place. Estate planners, then, have the opportunity to honor the mission of their social entrepreneur clients by utilizing the mechanisms within benefit corporation statutes to ensure the business’s social impact continues.

Future Trends & Opportunities:

Estate planning for social entrepreneurs is a completely untapped niche waiting to be occupied. Other future opportunities in social enterprise law may include litigating claims against directors and officers for breach of duty (and determining appropriate damages) and exploring other mechanisms and business models (such as the recently conceived social value enterprise, above) to advance social entrepreneurship. Exciting times!
SOCIAL MEDIA AND DISCOVERY

WHAT IS IT?
Social media, generally, refers to internet based technology that provides its users with a platform to share personal and/or professional information, ideas, interests and other forms of expression to a virtual audience; social presence builds real-life connections through the virtual communities and networks on social network site.

WHY NOW?
With social networks so pervasive, social media has infiltrated everyone’s lives, as people have adopted social media outlets as part of their daily routines and having instantaneous access via mobile apps (as opposed to desktop use). So, it should be no surprise that social media use is playing a significant role in federal and state court decisions. Recent case law confirms that social media content will continue to play a critical role during discovery and at trial, with evidence being introduced in all types of cases ranging from criminal prosecutions to tort liabilities to trademark infringement to sexual harassment to worker’s compensation, often having a devastating effect on the case.

KEY LEGAL ISSUES:
Social media presents unique issues obstacles that are not always adequately addressed with traditional E-discovery tools. While traditional discoverable ESI (such as records kept in course of business or emails) is stored and maintained a private computers or servers, cell or smart phones (e.g., text messages), or found in secure and time-stamped e-mails; thus, it is easier to access and authenticate. By contrast, social media is often cloud-based or stored on third-party servers, accessed through unique interfaces and both dynamic and collaborative in nature, it is more susceptible to alteration and fabrication.

Federal Rule of Evidence 902(13) & (14): amendments go into effect on December 1, 2017, particularly with 902(14) having significant impact on social media evidence collection processes, providing that electronic data recovered "by a process of digital identification" is to be self-authenticating, thereby not routinely necessitating the trial testimony of a forensic or technical expert where best practices are employed, as certified through a written affidavit by a “qualified person.” The Advisory Committee on Rules of Evidence (October 21, 2016) (http://www.uscourts.gov/sites/default/files/2016-10-evidence-agenda-book.pdf), explains that the purpose of the amendments is to ease the burden on authentication of electronic evidence, permitting authentication through submittal of a certification by a qualified person (e.g., forensic technology expert) without requiring
that person to testify in court; this shifts the burden onto the opponent to prove the information is inauthentic. FRE 902(13) relates to certified copies of machine-generated information, such as information obtained through your computer’s automatic registry (e.g., IP addresses stored when accessing websites) or a smart phone’s automatically stored data (e.g., GPS coordinates on dates and time). FRE 902(14) relates to certified copies of computer generated or stored information, which relates to obtaining copies of ESI (e.g., forensic copy of a smart phone, rather than using the phone itself).

**Discovery considerations:** Social media content is subject to discovery, despite the privacy settings imposed by the account user. State court practice varies, but most courts hold that social media is discoverable because there is no expectation of privacy; it is relevant and will lead to admissible evidence; and, there is no violation of any privilege. Some courts have permitted full access to private pages (see, e.g., Mazzarella v. Mount Airy #1, No. 1798 Civ. 2009, LLC2012 WL 6000678 (Ct. Com. Pl., Monroe Cnty., 2012); and Beswick v. North West Med. Ctr., Inc., 011 WL 7005038 (Fla. 17th Cir. Ct., 2011)); while others do not permit fishing expeditions and deny access if it deems that the claims are not inconsistent with the social media sought (see, e.g., Forman v. Henkin, 66 N.Y.S.3d 178 (N.Y. A.D. 2015); and Tompkins v. Detroit Met. Airport, 278 F.R.D. 387 (E.D. Mich. 2012)).

**Preservation and Collection:** Social media data (in a party’s “possession, custody, or control,” including legal authority and practical ability to access it) is subject to the same duty to preserve as all other types of ESI. This duty is triggered when a party reasonably foresees that evidence may be relevant to issues in litigation and failure to do so can result in sanctions. Preservation is important because you may not be able to subpoena user information from a social media platform which will invoke the Federal Stored Communications Act (SCA), which part of the Electronic Communications Privacy Act (18 U.S.C. §2701) as a defense to disclosure. There have been mixed results by the courts in whether or not a social media company must comply with a third-party subpoena (compare, e.g., Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010); and Facebook, Inc., et al., v. The Superior Court of San Francisco City and County, No. A144315, 2015 Cal. App. LEXIS 786 (Calif. App., 1st Dist. 2015), appeal pending at the California Supreme Court (Docket No. S230051); and Ledbetter v. Wal-Mart Stores, Inc., 2009 WL 1067018 (D. Colo. Apr. 21, 2009); and Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (Sup. Ct. 2010)). The general advise appears to be a subpoena with a narrowly tailored request and demonstration that production will reasonably lead to the discovery of admissible evidence.

**Authentication:** Practice under the Federal Rules of Evidence will substantially change under the amendments cited above when introducing electronic data; especially because the burden will shift to the opposing party (as opposed to focusing on the offering party). However, other forms of authentication will remain relevant (especially in state court practice). Authentication can be made through witness testimony of a personal with personal knowledge, circumstantial authentication through distinctive data, such as metadata or even email notifications, or testimony of a witness familiar with the scene depicted in the social media offered (e.g., a posted photograph). Without some form of supporting
circumstantial collaboration (e.g., verifying the hash values or witnesses familiar with the depicted posts), courts are routinely rejecting a “screen print” of a social media profile.

**Hearsay:** Status updates, public posts, chat transcripts, tweets, and more uploaded content lend themselves to novel uses of hearsay exceptions included present sense impressions, excited utterances, and then-existing mental, emotional, or physical conditions.

**Ethical consideration:** Collecting data from social media platforms can raise ethical concerns as the public or semi-public nature of SNSs allow litigants to collect data prior to discovery. An attorney or client (or their friends) may “friend” the account holder through a request. The Bar Association Ethics Committee has opined that an attorney may use their real name to send a friend request to the opposing party without disclosing the reason for making such a request. This follows for the attorney’s agent as well. Nevertheless, it is impermissible and improper for the attorney to assume a false identity to gain access to the opponent’s “friend page.” The New York City Bar states that “ethical boundaries to such ‘friending’... are not crossed when an attorney or investigator uses only truthful information to obtain access to a website, subject to compliance with all other ethical requirements.” A conservative Philadelphia Bar Association advisory opinion, however, requires that an attorney or agent also disclose the reason for making the friend request. It is suggested that the best practice in order not to taint evidence and destroy admissibility is to avoid “pretexting” or deceptive conduct when gathering information.

**Future Trends & Opportunities:** As Justice Kennedy opined that we cannot yet appreciate the full dimension and vast potential of cyber age, it is difficult to fathom the future trends of SNSs and its context in the legal world. However, it is safe to assume that states will follow the amendments set forth the Federal Rules of Evidence and adopt their own legislation regarding discoverability and introduction or SNS data in litigation. Moreover, new software will undoubtedly be developed in order to address preservation and collection efforts of SNS data. Judges, lawyers and parties must adjust their thinking so that SNS data is another type of ESI, and professionals should continue to educate themselves on the trends and innovations which help make this type of practice more accessible and affordable. Finally, other sources of electronic data - such as IoT (See IoT Section) will generate potentially relevant information for trial.
STUDENT LOAN LAWS

WHAT IS IT?

Generally speaking, there are two types of student loans: federal and private loans. See [https://studentaid.ed.gov/sa/types/loans/federal-vs-private](https://studentaid.ed.gov/sa/types/loans/federal-vs-private). Generally speaking, federal loans have more benefits than private loans: interest rates are lower and may be fixed, a borrower can temporarily defer payment while still in school or during the repayment term, and federal loans offer income repayment and loan forgiveness programs. However, not all students can qualify for federal loans, and with tuition skyrocketing, many have turned to the private market. With student debt on the rise, student loan law has become a specialty niche area of law practice, pioneered by lawyers like Joshua Cohen, Adam Minsky and Jay Fleishman. Student loan lawyers do more than simply assist with consolidation of loans; they can also help borrowers with anything from seeking loan discharge in bankruptcy or through other available avenues, avoiding default, stopping debt collector harassment and obtaining credit repair.

WHY NOW?

Student loan debt has now surpassed credit-card debt to become the second largest category of U.S. consumer debt (home mortgages being number one and the ability to own a home is ultimately impacted by the rising student loan debt). Approximately 43 million people have student loan debt with an average balance of $30,000; collectively being nearly $1.4 trillion by late-2016 ($108 billion is private student loans) or roughly 7.5% GDP. Many students face an impossible amount of debt, and, consequently, student loan debt is often cited as being one of the biggest modern financial crises.

College tuition has increased over the past several decades (though has grown at a lower rate in the last 10 years than previous decades), and research indicates that the increased reliance on student loans is a major factor in general cost increase. More than 70% of students require financial aid to attend school. Federal student loans are granted regardless of credit history (note: most students have no credit history), and approval is automatic if the student meets program requirements; however, PLUS loan approval is not automatic and credit history is considered. Federal loans are not priced and loan limits are not determined according to any individual measure of risk, but, rather, are politically determined by Congress; lack of risk-based decisions have been criticized as contributing to the inefficiency in higher education.

Finally, student loan debt and default increasingly have long term consequences. Both Ohio and Maryland have denied admission to applicants carrying significant loan debt, finding them unfit to practice. See [In Re: the Application of T.Z.A.O. for Admission](https://www.courts.maryland.gov/caselaw/download.cfm?caseid=9955002), Maryland Court of Appeals 2014 (affirming denial of admission) and
Law Grad Refused Admission for Student Loan Debt, National Jurist (2011). A recent NYT article reported that many states can seize professional licenses or suspend drivers licenses for borrowers who fall behind on student loan debt. See When Unpaid Debt Means You Can No Longer Work, NY 11/17/2017. In many ways, this penalty is worse than garnishment because it creates a vicious cycle: without a car or license, the borrower can’t work, and without income, the debt grows even larger.

**KEY LEGAL ISSUES:**

**Consumer protection and mishandling of loan payments:** Navient Corp., the nation’s largest student loan servicer that services more than $300 billion in federal and private student loans for more than 12 million borrowers (approximately 25% of the U.S.’s overall student loan borrowers) is currently facing four (4) lawsuits alleging that it harmed student loan borrowers throughout the repayment process. In January 2017, the Consumer Financial Protection Bureau filed suit seeking, inter alia, compensation to harmed borrowers, claiming that, since at least January 2010, Navient misallocated payments, steered struggling borrowers toward multiple forbearances instead of income-driven repayment plans, and provided unclear information about how to re-enroll in income-driven repayment plans and how to qualify for a co-signer release. In August 2017, the U.S. District Court judge denied Navient’s motion to dismiss (see Consumer Fin. Prot. Bureau v. Navient Corp., Case No.: 3:17-CV-101, 2017 U.S. Dist. LEXIS 123825 (M.D. Pa. Aug. 4, 2017), and the case will proceed to discovery. In January 2017, the Illinois and Washington Attorney Generals, and in October 2017, the Pennsylvania Attorney General filed suits against Navient making similar claims to the CFPB suit, and also alleging that Navient, when it was part of Sallie Mae (through 2014), made subprime loans to students, particularly those attending for-profit schools.

**Loan Forgiveness** - Federal student loans (note: not private) can be administratively discharged for total and permanent disability under the HEOA, when the borrower has lost "substantial gainful activity" (SGA) as a result of the disability (as opposed to inability to earn income). Starting in 2013, the borrower can use Social Security Administration determination of disability as proof if placed on a five- to seven-year review cycle (the longest SSA review period). Teachers in specific critical subjects or in schools with more than 30% of its students on reduced-price lunch (a common measure for poverty) can qualify for federal loan forgiveness up to $77,500. In addition, any person employed full-time (in any position) by a public service organization, or serving in a full-time AmeriCorps or Peace Corps position (PLSF, signed by President Bush in 2007) qualifies for federal loan forgiveness after 10 years of 120 consecutive payments without being late. The IRS considers any loan forgiveness or discharge is considered as taxable income pursuant to 26 U.S.C. § 108(f).

**Discharge** - As of August 2016, the Department of Education received over 98,000 complaints from students about fraud, with 98.6% related to for profit schools. See http://www.chicagotribune.com/business/ct-biz-student-loan-fraud-claims-20171110-story.html Student loan discharge may be available if a borrower was a victim of fraud or if the school shut
down. See Pursue a Federal Loan Discharge as a Victim of Fraud, US News & World Report (12/9/2015) - though it may become more difficult to do with changes underway by the Trump Administration.

Debt Collection - student loans become immediately due (principal and interest) upon default. The DoE will request a Treasury offset, whereby the TRE to withhold federal income tax refunds, Social Security payments (including disability benefits), and other federal payments, all to be applied to the defaulted loan. In some cases, state-issued licenses, including driver’s licenses, may be withheld, and up to 15% of disposable pay may be garnished through the debtor’s employer. At times, the federal loan may be referred to a debt collector, and, this type of debt collection is the only option available for private loans. Previously, debt collectors could not call cell phones without permission; however, Congress recently gave debt collectors the right to use robocall technology to autodial federal student loan borrowers who haven’t made their payments.

Lawsuits for debt collection, while not very common, do happen. For example, between November 2012 and April 2016, Transworld Systems filed 95,000 lawsuits across the nation to collect unpaid loans on behalf of National Collegiate Student Loan Trusts (holder of approximately 11% of private student loan debt). Most of these lawsuits were dismissed on the basis that there was faulty paperwork and false and misleading affidavits to support collection; with commentators likening the suits to the robo-signing during the mortgage crisis (e.g., thousands of foreclosure lawsuits filed without reviewing the underlying paperwork). In September 2017, Consumer Financial Protection Bureau filed separate complaints against both Transworld and NCSLT for illegal collection methods, resulting in a settlement of $21 million payment in penalties and fines to the TRE, and the appointment of an independent auditor to review all student loans to proper documentation without such, they must cease collections and provide additional restitution. As a result, Navient stands to lose approximately $5 billion in student loans as a result of improper documentation.

Bankruptcy - The only way to discharge student loans is through bankruptcy, but these loans are considered practically non-dischargeable since the standard is generally difficult to meet and most cannot afford an attorney or additional litigation costs associated with such proceedings. However, the debtor must initiate an adversary proceeding (i.e., separate lawsuit) within the bankruptcy proceeding and must show “undue hardship” in the context of 11 U.S.C. § 523(a)(8)(B). The standard to meet “undue hardship” varies between jurisdictions, but most circuits apply the three-prong Brunner test: (1) debtor cannot maintain, based on current income and expenses, a “minimal” standard of living for self and dependents if forced to repay the loan(s); (2) additional circumstances exist indicating this state of affairs is likely to persist for a significant portion of the repayment period of the student loans; and (3) the debtor has made good faith efforts to repay the loans. See, e.g., In re Pena, 155 F.3d 1108, 1111 (9th Cir. 1998); Bryant v. Pa. Higher Educ. Assistance Agency (In re Bryant), 72 B.R. 913 (Bankr.E.D.Pa.1987); N.D. State Bd. of Higher Educ. v. Frech (In re Frech), 62 B.R. 235 (Bankr.D.Minn.1986); Marion v. Pa. Higher Educ. Assistance Agency (In re Marion), 61 B.R. 815 (Bankr.W.D.Pa.1986).
**Future Trends & Opportunities:** Higher education is big business, and the cultural basis starting the 1970s-80s was a “college-for-all” mentality has led students to apply in droves to colleges and universities seeking educational opportunities that have not translated into guaranteed employment; leading to the debt crisis facing the population today.

It is unlikely that the government will move into a free higher education system (at least in the nearer future), and Congress is set to re-authorize the HEOA (which expired in 2014, with some programs having automatic extensions until new reconciliation or reauthorizing legislation is introduced). Under the Trump Administration, a new system is set to be introduced in 2019; and it is expected that Congress will no longer give preference to Nelnet, Great Lake, Navient and American Education Services, which would shift a significant share of business to, possibly, nonprofit companies like Missouri Higher Education Loan Authority and Oklahoma Student Loan Authority. Other expected reforms include ending the Graduate PLUS loan program, with Republicans thinking that graduate school borrowing should be pushed into the private market entirely.

For several years, the Obama Administration and Democrats proposed capping the PSLF program at $57,500, and Republicans proposed eliminating the program all together. The Government Accountability Office predicts that the cost to taxpayers for the PSLF program alone will be more than $80 billion. It is expected that the Trump Administration will heavily reform the program for qualifying fields (including refining the definition of working for a nonprofit for doctors and attorneys) and adding the aforementioned cap. Additionally, there is bi-partisan agreement that the current federal financial aid system is too complex for families, and there needs to be significant reforms to income-driven repayment plans.

A practical response to avert further student loan debts is the push of vocational education. On June 15, 2017, President Trump signed an executive order aimed at addressing an apparent skills gap that has contributed to more than 6 million domestic vacancies that employers are struggling to fill; calling on businesses (and the Department of Labor) to increase their apprenticeship offerings, and promoting schools and community colleges to communicate more with employers and recruiters outside of academia to ensure students are gaining the marketable skills and training they will need after graduation. States have also taken this approach. California, for example, is spending $6 million on a campaign to revive the reputation of vocational education, and $200 million to improve the delivery of it.

With loan forgiveness plans cut, and vocational programs on the rise (themselves with a checkered past with regard to student loan fraud), student loan law is a practice area that will continue to be in demand.
WHAT IS IT?

According to Wikipedia: “The tiny house movement is a description for the architectural and social movement that advocates living simply in small homes. There is currently no set definition as to what constitutes as a tiny house; however, a residential structure under 500 square feet is generally accepted to be a tiny home.” Tiny houses can be stationary (referred to as “accessory dwelling units”) or mobile (i.e., recreational vehicles).

WHY NOW?

The tiny house movement has taken off in recent years, partly as a reaction to the Great Recession, and partly as a result of a cultural trend towards more ecologically sustainable lifestyles.

KEY LEGAL ISSUES:

Tiny houses may be tiny, but they can raise giant legal questions. These include (1) whether a renter can construct a tiny house consistent with his or her lease; (2) whether a member of a homeowners’ association (“HOA”) can construct a tiny house without violating the association’s covenants; (3) whether zoning law permits the construction of a tiny house; and (4) whether the tiny house complies with the relevant building code. Specific to mobile tiny houses are issues such as (1) whether the vehicle complies with fire and safety criteria and (2) where the owner can legally park the vehicle. As tiny houses gain popularity, they face increasing opposition from neighbors who argue that tiny house developments violate existing zoning laws and can lead to diminution of home values. See Tiny Houses Trendy Unless They Go Nextdoor, USA Today (11/14/2017).

Some churches have constructed tiny houses for homeless and lower income families. But a Tennessee church was denied zoning for a micro-housing development (See Tennessee.com (8/7/2017), as was a South Carolina church, which brought suit in response to a zoning board denial. Lawsuit Between City and Church Involving Tiny House Resolved (10/2/2017)(settlement of church’s lawsuit under religious freedom law against City for denying request to church for zoning permit to site tiny house for homeless).
Future Trends & Opportunities: The law hasn’t kept pace with the increased popularity of tiny houses. They don’t comply with most building codes which aren’t designed for facilities with 5 foot ceilings or limited floorspace. Consequently, there have been proposals to change building codes to make them compatible with tiny houses (see Legal Tiny Houses, Fine Home Building (11/2/2016). The Tiny House Association tracks proposed regulations and offers opportunity for input. Moving forward, lawyers may be needed to assist with changing the law as much as with ensuring compliance and zoning laws.
WHAT IS IT?
Vaping is the act of inhaling vapor produced by an electronic cigarette or similar device. Vaping devices include not just e-cigarettes, but also vape pens and advanced personal vaporizers (also known as 'MODS'). Generally, a vaping device consists of a mouthpiece, a battery, a cartridge for containing the e-liquid or e-juice, and a heating component for the device that is powered by a battery. When the device is used, the battery heats up the heating component, which turns the contents of the e-liquid into an aerosol that is inhaled into the lungs and then exhaled. The e-liquid in vaporizer products usually contains a propylene glycol or vegetable glycerin-based liquid with nicotine, flavoring and other chemicals and metals, but not tobacco. See The health risks of e-cigarettes are uncertain. They are likely safer than tobacco cigarettes, but there is also a growing body of evidence that some of the chemicals being inhaled may be dangerous. Source: Center on Addiction.

WHY NOW?
Electronic cigarettes were first sold around 2004, but usage — as a replacement or supplement to tobacco cigarettes — has grown dramatically as the dangers of smoking have become well-known. The global e-cigarette market — worth $9.5 billion in 2017 — has been forecast to attain a value of $48 billion by 2023. Source: Business Wire (March 2018). Companies like Juul which develop and manufacture e-cigarettes have had runaway success; Juul holds 68 percent of the e-cigarette market and is currently raising $1.2 billion in funding to broaden distribution globally. Source: Fortune. (June 30, 2018).

More recently, e-vape producers have added mouth-watering flavors like strawberry milkshake and cinnamon rolls to e-cigarettes making them more effective as a substitute for tobacco cigarettes but also more appealing to minors. Source: Philly Voice.

KEY LEGAL ISSUES:
Vaping raises interesting legal issues for several reasons. First, because vaping is generally viewed as a lesser evil than, and a substitute for tobacco smoking, many fear that onerous regulation of vaping will increase costs and availability and make it a less attractive alternative for smokers. Second, in many states, the rise of vaping has coincided with the legalization of marijuana, leading to questions over whether vaping shops and products should be treated similarly to those for cannabis.

FDA Regulation - In 2016, the Federal Drug Administration (FDA) finalized a rule extending its regulatory authority to all tobacco
products including e-cigarettes. The rule requires health warnings on roll-your-own tobacco, cigarette tobacco, and certain newly regulated tobacco products such as e-cigarettes and also bans free samples. The new rule also restricts youth access to newly regulated tobacco products by: 1) not allowing products to be sold to those younger than 18 and requiring age verification via photo ID; and 2) not allowing tobacco products to be sold in vending machines (unless in an adult-only facility). See FDA Website.

The rule also requires e-cigarette to file with the FDA to show that the products meet the applicable public health standard set by the law and receive marketing authorization from the FDA. Implementation of these approval requirements has been delayed until 2022 to allow the FDA to continue to study risks related to e-cigarettes as well as their role in reducing cigarette smoking. FDA Announcement (2017).

**First Amendment Concerns** - By treating e-cigarettes like other tobacco products, the FDA’s regulations also subjects e-cigarettes to more onerous advertising regulations. A recent lawsuit by the vaping industry alleges that these advertising restrictions are unconstitutional prior restraints on speech in violation of the First Amendment. See The Hill (January 2018).

**State & Local Regulation** - Though the safety of e-cigarettes is regulated by the federal government, state and local authorities have broad authority over when and where vaping can take place. Again, with state and local regulations, legislators are often deciding whether to treat vaping like smoking. Thus, recent actions include Springfield, Massachusetts proposed ban on vaping in public places, San Francisco’s ban on flavored vaping products, New Orleans’ ban on vaping in bars and New Jersey’s consideration of increased taxes on vaping products.

A comprehensive list of all state laws related to vaping is available at the Public Health Law Center.

**Future Trends & Opportunities** - As the vaping industry grows, it will create opportunities for lawyers to assist in advising on and navigating existing and potential regulation. Lawyers with real-estate or zoning practice areas may also find a market in representing vaping shops or municipalities zoning board hearings related to vaping operations. Finally, defects in vaping hardware (such as exploding cigarettes) may open the door for class actions and tort and product liability lawsuits that will require specialized knowledge of how these products work.