NEW LAW ANTHOLOGY

A collection of articles from Law Practice Today, featuring exclusive extended content.

Compiled by Daniel Lear and Stephen Embry, with Nicholas Gaffney

Foreword by Andrea Malone

www.lawpracticetoday.org
Welcome...

Welcome to the inaugural Law Practice Today New Law Anthology. This anthology has been compiled for a dual purpose: To illuminate the many ways in which legal professionals are staying on the cusp of technology and innovation, and to help you gain a better understanding of these developments. In 2016, Law Practice Today editors and authors Daniel Lear, Stephen Embry, and Nicholas Gaffney both wrote and sourced incredible articles detailing technology, innovation, and thought leaders within the field. We decided to honor them and our contributors by presenting the "best of the best" articles in this cohesive and commemorative manner.

In this anthology, you'll learn about a wide variety of issues. Get in-depth takes on emerging practice areas such as robot law and cannabis law, learn the legal side of cultural trends such as drones and Bitcoin, read interviews with some of new laws' pioneers, and much more.

We would like to extend thanks to Dan, Steve, and Nick for their efforts, to the featured authors for their exemplary articles and expertise, and to the Law Practice Today readers who demonstrated such a passionate interest in these topics.

Regards,
Andrea Malone, Editor-in-Chief of Law Practice Today
About the Editors

Daniel Lear is a lawyer, blogger, and legal industry gadfly. As a technology-focused business lawyer, Dan advised a range of companies, from startups to the Fortune 100, on developing agreements and terms for early cloud service offerings well before "the cloud" was an everyday norm. In 2014, Dan joined Avvo, an online legal marketplace, where he is the Director of Industry Relations and frequently speaks to lawyers and bar associations. Dan has been mentioned, featured, or published in the ABA Journal, Law Practice Today, Law Technology News, NWLawyer, Above the Law, and other legal industry press. In 2014, Dan was honored with the Washington State Bar Association President's Award for his participation in, and advocacy of, legal technology projects locally and nationally. In 2015, he was named to the FastCase 50—a group of entrepreneurs, innovators, and trailblazers in the legal profession. Find him on Twitter at @rightbrainlaw or on the web at rightbrainlaw.co.

Stephen Embry is a member of Frost Brown Todd LLC and is a member of the Firm's class action and privacy groups. He frequently defends participants in consumer class action litigation and mass tort litigation. Stephen is a national litigator and advisor who is experienced in developing solutions to complex litigation and corporate problems. His mission is to find simple, successful, and elegant solutions to the problems posed by complex and substantial civil litigation, primarily in the mass tort and consumer class actions, and privacy and data breach arenas. Find him on Twitter @sembry244 or on LinkedIn.

Nicholas Gaffney is a lawyer and former journalist, and has helped lawyers and other professionals creatively communicate the value of their services for the past 20 years. The Wall Street Journal took notice and called him a "marketing guru." An expert at crafting winning strategies that achieve clients' business goals, he has a particular expertise in litigation and crisis communications. His work has been recognized nationally with his firm, Zumado, being named one of the top PR and Crisis Communications Firms in the legal industry. Nick is committed to giving back to the legal profession by actively participating in the ABA's Law Practice Division; all of the interviews included within this anthology have been facilitated and conducted by him.
## Table of Contents

- Insights of a New Law Pioneer ... 4
- Seven Things Every Lawyer Should Know About Drones in 2016 ... 6
- Making It Rain: Updates on Crowdfunding Law ... 12
- The Brave New World of Robot Law ... 16
- Crowdsourcing Better Access to Justice ... 20
- The Future Is In Our Hands: Biometric Identification As Authentication ... 23
- The Internet of Things: Ubiquitous Legal Issues ... 26
- Weary of Wearables: IP, Privacy, and Data Security Concerns ... 31
- The Resurgence and Relevance of Bitcoin: What You Need to Know, and Why ... 37
- Integrative Law: Evolution of the Legal System ... 40
- Bringing Creativity to Legal Operations ... 45
- How to Become a Cannabis Attorney ... 47
- Cyber Insurance: Panacea or Pandora's Box? ... 50
- Using Informatics to Drive Process Improvement ... 55
Insights of a New Law Pioneer

With Richard Granat, by Nicholas Gaffney

Richard Granat is a new law pioneer. He created one of the first virtual law firms in the country in 2002 in Maryland, which led to the establishment of DirectLaw—a client-centric virtual law firm platform for solos and small law firms. He was the co-chair of the eLawyering Task Force of the Law Practice Division for many years, and was awarded the ABA’s Louis M. Brown Lifetime Achievement Award for Legal Access and the James Keane Award for Excellence in eLawyering.

In 2009, the ABA Journal recognized Richard as one of 50 Legal Rebels throughout the United States—individuals who are engaged in changing the legal profession. Richard is co-director of the Center for Law Practice Technology at Florida Coastal School of Law, which has developed an online curriculum in law practice management for law students nationwide.

Nicholas Gaffney (NG): What projects or ideas have you been focusing on recently?

Richard Granat (RG): A network version of DirectLaw, so that a manager can coordinate and manage cases for a network of virtual lawyers. We are implementing this first in the public sector, with a network of pro bono lawyers in New Mexico and Massachusetts. We have just launched the network version of DirectLaw for private law firms that are working together collaboratively. We think that networks of virtual lawyers serving clients nationwide will continue to evolve, and our platform is designed to manage and support these networks.

NG: What could lawyers look at in a new way that would benefit their clients and society?

RG: A big challenge for solos and small law firms is to figure out how to serve the latent market for legal services—the approximately 80% of US consumers who can't afford today's legal fees. One solution is to offer software-powered unbundled legal services online for a fixed fee. This kind of service is scalable, and can generate net revenues which are comparable to typical hourly billing rates of solos and small law firms.

NG: What one thing about the practice of law would you change if you could?

RG: For consumers, moving away from the "job shop" business model with hourly billing rates towards the "value-chain" business model with fixed fees for discrete legal services.

NG: What is the most exciting development you have seen recently in the practice of law?
RG: The "unbundling legal services and online delivery," as it's the path towards the "value-chain business model" and opening up service to the latent legal market.

NG: What technologies, business models, and trends do you think will have the biggest impact on the practice of law over the next two years?

RG: Solos and small law firms will incorporate into their web sites a secure client portal to enable them to work with the clients online securely and confidentially.

Software as a service (SaaS) legal applications will continue to evolve, enabling software-powered legal services that manage the details better than a person.

Web-enabled document automation is a good example of an application that creates a first draft of a document instantly from the client's answers to questions in an online questionnaire for the lawyer's further review, revision, and analysis. Software-powered legal services enable lawyer's to practice law at the "top of their license," devoting more time to analysis, counseling, negotiating, and advocacy.

NG: What's the best new law practice management idea you have heard recently?

Rg: CMS (client management systems) that are integrated with a law firm's web site to help the law firm manage and nurture the flow of leads and unique visitors hitting the web site.
Seven Things Every Lawyer Should Know About Drones in 2016

By Stephen Palley

Once the stuff of science fiction or restricted to military use, drone technology has gone mainstream. News reports are full of stories about how drones are being used, or misused, for commercial and recreational purposes. Let's take a 1,000-foot view of seven key issues for lawyers to consider, to help the majority of practicing lawyers who are not FAA regulatory specialists with basic issue spotting. (It is not intended to be an authoritative primer on drone regulations or FAA practice.) We'll also get an "in the trenches" perspective from Suffolk Construction's general counsel, Wendy Venoit, who recently obtained FAA approval for her company's drone use.

1. Drones are "Aircraft"

While awareness has increased dramatically in the last 12 months, some businesses may still need to be reminded that the fact that they can purchase a drone for $1,000 does not mean that it can use it without going through the FAA approval process.

We'll start simple. Drones are "aircraft" under federal law. Their use and regulation are governed by the FAA. A business can't just purchase a drone on Tuesday and start (legally) using it on Wednesday without first seeking and receiving FAA approval. The fact that drones are inexpensive and easy to purchase does not change the existing legal framework governing their use (more on that below). They must now be licensed and registered, whether used for recreational or commercial purposes. In addition to the feds, a number of states have passed or are considering passing drone-related legislation.

2. Getting Permission

There's a difference between recreational/hobby drone and commercial drone use. The FAA provides general guidance on this. The bottom line is that if you use a drone for your business, you must petition for what's known as a "Section 333" exemption in order to fly it. That's true whether or not you charge an additional fee for using the drone.

Until recently, "recreational" users did not have licensing or registration obligations. That has changed. A recreational user who buys a drone for non-business purposes must now register their drone with the FAA and pay a $5 licensing fee (as of December 21, 2015). The FAA has partnered with the Association for Unmanned Vehicle Systems International (AUVSI) and the Academy of Model Aeronautics (AMA) to develop a website, knowbeforeyoufly.org, which provides information on recreational drone usage, including registration requirements and restriction on use. (Some examples: don't fly
your drone over 500 feet, in restricted airspace [Washington, D.C. is off limits] or within 5 miles of an airport.)

3. Tort Law Hasn't Been "Disrupted"

Whether or not drone technology is "disruptive," drones and drone operators live in an existing legal framework with established rights, remedies, and liability, both civil and criminal. The news is full of reports of drones falling from the sky and injuring people or going places where they weren't supposed to go.

While the technology may be complex, the law seems fairly straightforward. There's no "drone exception" to negligence claims, as far as we're aware. Whether someone is injured by a drone or injured by a negligently operated crane, common law tort remedies still apply. Criminal laws do too.

4. Drone Data is Not Free

Drones may be able to capture petabytes of useful data at a fraction of the cost of a helicopter. But fast and inexpensive data acquisition can be both a benefit and a liability. As one commentator explains: "Actionable insight is an asset. Data is a liability. And old data is a non-performing loan."

First, the benefit. Consider the following quote from a recent article in the MIT Technology Review titled "New Boss on Construction Sites is a Construction Drone," which explains how drone data can be used to help identify factors that may be causing schedule delays on a construction project:

"We highlight at-risk locations on a site, where the probability of having an issue is really high," says Mani Golparvar-Fard, an assistant professor in the department of civil engineering at the University of Illinois, who developed the software with several colleagues. It can show, for example, that a particular structural element is behind schedule, perhaps because materials have not yet arrived. "We can understand why deviations are happening, and we can see where efficiency improvements are made," Golparvar-Fard says.

This is one of the many useful applications of a construction drone: tracking progress and identifying potential delays. But it's easy for a lawyer to war-game risks that come with the benefit of being "understand why deviations are happening." What else are you capturing? And what are you doing with that data?

A hypothetical illustrates the trade-off. Assume a visitor to a construction site trips and falls into a trench that was allegedly improperly guarded, and lacked proper warnings. Is the exposure worse if two months of drone footage showed the site wasn't scrutinized and nothing was done? (Or assume it was scrutinized and nothing was done—take your pick).
This isn't completely uncharted territory. Cameras have been used on and in construction sites for years. However, the access and amount of data that drone technology can provide is unprecedented, as is the apparent up-front cost, at least for now.

5. The Insurance Landscape Remains Uncertain

Legacy insurance products may or may not apply to drone-related losses. The industry is working to create new products, but it's a mistake to assume that all drone operations will be covered by existing policies.

How might a company’s existing insurance policies apply in the event of a drone-related loss? Assume that (1) a general contractor uses a drone to monitor an active construction site, and that operator error (2) causes the drone to fly off the site and crash into a moving car on an adjacent street injuring the car and its occupants. The occupants and owner sue the GC (we'll keep it simple and assume that they don't drag in the owner, subcontractors, product manufacturer, etc). Is it covered or not?

One of the standard CGL policy forms excludes coverage for: "'Bodily injury' or 'property damage' arising out of the ownership, maintenance, use or entrustment to others of any aircraft, 'auto' or watercraft owned or operated by or rented or loaned to any insured. Use includes operation and 'loading or unloading.'" This exclusion is subject to an exception for "Liability assumed under any 'insured contract' for the ownership, maintenance or use of aircraft or watercraft["]"

In our fact pattern (where the GC alone was sued) the "insured contract" exception is probably not going to help. An insurer might argue that a drone is an "aircraft", that the exception does not apply, and that there's no coverage. Whether or not the insurer is correct or has a duty to defend will depend on the specific allegations in the lawsuit and applicable state law: one exclusion isn't necessarily the end of the inquiry, but it could certainly be a problem if coverage was expected.

Might other policies apply: Aviation? Drone policies? Property? Other products? It really depends. You can find a more extended discussion of this subject here.

For now, whether or not a client is using drones in their business or considering a new drone program, it makes sense to review applicable insurance programs to evaluate adequacy and availability of coverage. Existing policies may need to be modified to provide greater assurance of coverage, and additional policies put into place, and new types of coverage considered.

6. Industry Perspective

To provide a fresh perspective on the FAA exemption process, we interviewed Wendy
Venoit. Ms. Venoit is general counsel of Boston-based Suffolk Construction, listed as the 31st largest construction company in the United States by trade publication *Engineering News Record*. She joined the company in early 2015 after spending the bulk of her career in private practice as a partner in the construction law practice at Connecticut-based Pepe & Hazard and McElroy, Deutsch, Mulvaney & Carpenter, LLP. Suffolk recently received FAA approval of its exemption request, and we asked for her thoughts and feedback on the process.

**Stephen Palley (SP): Why did Suffolk choose to go through the exemption process? Was it a lawyer-driven initiative or a business initiative? Or both? Was it something that customers demanded?**

Wendy Suffolk (WS): As it is unclear when the FAA will finalize the rules on the commercial use of drones, the exemption process was necessary to ensure that Suffolk was able to utilize drones on its projects within the guidelines set by FAA as soon as possible. Implementing the use of drones on Suffolk projects is consistent with Suffolk's goal to balance its strong safety program with the increasing need to implement innovative processes to construct its projects, and was driven largely by the project teams. The choice to pursue a letter of exemption from the FAA and comply with FAA rules and regulations which ensure that the operation of the drones was within approved parameters was the responsibility of the legal department. Suffolk assessed the benefits of drones from a job site safety perspective and sought to comply with the FAA regulations so that drones could be utilized as an effective part of the safety program.

**SP: When did Suffolk do this? How long did it take? Is the process complete?**

WS: Suffolk began the exemption application in July 2015 and was issued an exemption letter by the FAA in early November 2015. It took a little under 90 days from submitting the application to getting a decision from the FAA. The exemption granted by the FAA has several requirements prior to and during the operation of a drone.

**SP: Were you able to do it in-house or did you need to go to outside lawyers?**

WS: We were able to handle the exemption process in-house.

**SP: Any useful resources that you discovered on the way?**

WS: A lot of material is available on drone use and the potential implications of the FAA rule, but most anticipates the impact of rule or how the FAA will enforce and regulate the use of drones. However, as all exemption applications and decisions are on the FAA docket, reviewing prior applications for exemptions was the most useful resource in preparing our own application.
SP: Any unique "gotchas" to be aware of, beyond the exemption process?

WS: No "gotchas" per se, but the exemption is not a carte blanche to operate the drone at will and has some strict requirements, which could pose a challenge for many companies.

SP: Are most of your competitors also going through the process or are you still in the vanguard?

WS: Most larger construction companies appear to recognize the utility of operating drones, so several have applied and been granted the exemption.

SP: How prevalent do you expect drones to be in the construction industry in the next five years?

WS: Drones could minimize the risks associated with inspections of hard to reach areas, and assist in the elimination of conflicts during construction. As such, it will be an asset in keeping people safe while increasing efficiency, so I expect that drone use will be prevalent in construction in the next five years.

SP: In addition to exemption process and licensing, how (if at all) has issue of drone usage come up in contract negotiation?

WS: It's not a significant contract issue, but developers and owners want technology to be used and drones are on the leading edge of technology and getting a lot of publicity. It is a benefit for Suffolk to be able to offer the use of drones as part of innovative technologies and its safety program for its projects. It is anticipated that owners/developers will address certain issues in the contract as drone use becomes more prevalent. Specifically, it is expected that there will be certain contractual provisions regarding indemnification for injury, property damage and unauthorized use, insurance and compliance with the FAA guidelines.

7. What Next?

Drones are here to stay, whether we like it or not. The benefits that they offer must be understood within an existing legal framework. For hobbyist/recreational users, following registration requirements and familiarizing oneself with use limitations are a good first step.

For lawyers advising businesses considering a drone program, a good place to start may be with some standard "W" questions: What will you be using? Who will use it? When will you start? When will you end? What data will be gathered? Who will own the data? Why will the data will be gathered? Where will it be stored? What insurance will be available if there's a problem with the drone? Those questions will surely lead to
others, and a plan for safe takeoff can be created.

About the Author

Stephen Palley is a trial lawyer in Washington, D.C., and the founder of Palley Law, PLLC. He focuses his practice on insurance coverage, construction law, and emerging technology. Follow Stephen on Twitter @palleylaw.
Making It Rain:
Updates on Crowdfunding Law

By Amy Wan

In the precursor to this article, "New U.S. Crowdfunding Rules Offer High Hopes for Capital Formation," I briefly introduced the three main regulations legalizing crowdfunding. This article intends to provide an update on the state of crowdfunding law and the crowdfunding industry today.

One Year Anniversary of Regulation A+

Regulation A+, which revamped its predecessor Regulation A, became effective on June 19, 2015—just over a year ago. Regulation A+ provides an exemption from registration for non-Exchange Act reporting companies for public offerings of up to $50 million in securities in any 12-month period. The exemption allows non-accredited investors to purchase the securities of private companies. Previously, Regulation A only allowed companies to raise up to $5 million in securities in any 12-month period which, coupled with bureaucratic and uncoordinated state and federal review processes, often proved too inefficient and expensive a mechanism for raising capital when compared with the fundraising cap.

Since Regulation A+ become effective, Regulation A+ filings have been on the upswing. Between 2006-2013, fewer than 30 Regulation A filings were submitted to the SEC each year—and even fewer filings ever completed the lengthy qualification process. In the first twelve months of the new Regulation A+, over 100 filings under Regulation A+ have been publicly filed to date. That number, however, is likely a dramatic underestimate, since many issuers file their offerings confidentially. Of those filings, approximately 44 offerings have been qualified by the SEC, with 16 offerings actively selling today.

Previously, an issuer would expect the qualification process to take upwards of a year or two—and many issuers subsequently abandoned their offerings for this reason. Under the revamped rules, issuers take an average of 109 days to qualify a Reg A+ offering from the date of filing. Note, however, that this number is not precise. Some issuers have filed their offerings prior to the June 19 effective date but qualified after the effective date, and then amended their offerings under the new rules, which slightly skews the average.

First Quarter Results of Regulation Crowdfunding

Regulation Crowdfunding, also known as Title III or Reg CF for short, enables companies to raise up to $1M from non-accredited investors. The regulation became
effective on May 16, 2016. Previously, only accredited investors who met certain financial requirements were eligible to back businesses in this manner.

In the first three months of Regulation CF's effective date, a total of 107 offerings have been filed. As of the time of writing, 17 of those campaigns totaling over $5 million in commitments have reached their minimum investment goals.

Notably, Regulation CF issuers have been creative in the securities they've been offering. Instead of traditional debt or equity offerings, nearly half offer either SAFE or CrowdSAFE securities. The SAFE, or Simple Agreement for Future Equity, is a security instrument popularized by a leading San Francisco-based accelerator Y-Combinator. AngelList spin-off Republic iterated on the investment vehicle by introducing the CrowdSAFE, which purports to solve several issuers.

Unresolved Issues with Regulation Crowdfunding

Even prior to its effective date, many industry experts criticized the burdensome requirements associated with Regulation CF. To combat some of these issues, Congressman McHenry has introduced proposed legislation called the Fix Crowdfunding Act (HR 4855) that passed a vote by the House of Representatives, but has yet to receive a vote at the Senate. HR 4855 makes the following changes:

SPVs to Consolidate Cap Tables

Under the current rules, Regulation CF does not allow for special purpose vehicles (SPVs). The proposed HR 4855 included amendments to the Investment Company Act to enable companies to use SPVs for more efficient capital raising.

SPVs allow issuers to consolidate multiple investors into one entity. Typically, an issuer negotiates terms with a lead investor and any other investor wanting to join the funding round does so on the same terms as the lead investor. These follow-on investors will buy equity in an SPV, which becomes the one consolidated investor in the company. This way, issuers can avoid having to manage tens or hundreds of investors on their cap table, chase around individual investors, and can spend more time working on their business rather than dealing with the administration and management of individual investors. Anecdotally, venture capitalists are said to shy away from companies with lengthy cap tables.

The amended bill passed by the House Financial Services Committed amends the Investment Company Act to specifically permit the use of an SPV structure for conducting a Title III offering; however, the use of an SPV (which is defined in the amended bill as a "crowdfunding vehicle") must meet the following eight (8) additional qualifying conditions:

- The purpose of the SPV must be limited to the acquisition, holding and disposition of the securities of a single issuer;
● The SPV must receive no commission in connection with the acquisition, holding and/or disposition of the subject issuer securities;

● No person acting on behalf of the SPV may receive any commission in connection with the acquisition, holding and/or disposition of the subject issuer securities, unless they are a registered investment adviser (RIA);

● The SPV may issue only one class of securities;

● The SPV and the issuing company are deemed to be co-issuers of the securities sold under Title III;

● The SPV is current in its reporting obligations under Rule 202 (17 C.F.R 202);

● The issuer company is current in its reporting obligations under Rule 202 (17 C.F.R 202); and

● The SPV is advised by a registered investment adviser (RIA).

Removing Future Public Registration (or the 12(g) problem)

The proposed HR 4855 removed a provision requiring companies to register and begin reporting under the Exchange Act, similar to that of a public company, within 2 years of exceeding $25 million in assets if the company has 500 or more non-accredited investors. However, the amended bill approved by the House Financial Services Committee includes the exemption except for issuers who, as of the last day of any fiscal year, have: (a) a "public float" (calculated as the # of common shares/equity units outstanding × last sold price) of < $75 million; or (b) if the public float amount is $0, annual revenues of < $50 Million.

Other Issues

The following solutions were proposed in HR 4855, but were not part of the amended HR 4855 approved by the House of Representatives:

● **Testing the Waters:** Issuers would be able to solicit interest prior to actually spending money on lawyers and accountants. Given that companies must brace themselves for the scenario in which they cannot cover transaction costs or loss money and time as a result of not having raised enough funds, the ability to gauge investor interest up front may save a number of issuers from being in the red on day one (and may encourage other companies to boldly steam forward).

● **Raising the Funding Cap From $1M to $5M:** Onevest/1000 Angels Chairman Alejandro Cremades wrote that "nowadays startups on average raise, at a Seed stage, in the neighborhood of $2M+. The fact that startups will have a limit of $1M per year will either force them to be under-capitalized or conduct another type of offering in parallel to raise the remaining capital from accredited investors, which means more costs from a legal perspective." Raising the funding cap to
$5M would make the transaction costs more justifiable and allow companies to raise the capital they need.

- **Portal Liability:** Funding portals are the gatekeepers against fraud. To combat fraud, many funding portals plan to conduct due diligence on issuers and curate the campaigns they accept on their platforms. However, whereas Title II portals are not liable for information provided by issuers, Regulation CF funding portals have significant liability for misstatements or omissions of the issuer. The SEC expresses does not preclude private rights of action against funding portals, making them a prime target of plaintiff's counsel for deals that go sideways—especially if the issuer is no longer around. Many would like to see a proposal that requires certain due diligence and verification, and adds language to clarify that funding portals will not share in issuer liability unless they *knowingly* make an untrue statement, omit material facts, or engage in fraudulent or deceitful conduct.

**About the Author**

Amy Wan, Esq., CIPP/US is a Partner with CrowdfundingLawyers.net, where she practices crowdfunding law. Formerly, she was general counsel at Patch of Land, a real estate marketplace lending platform. While there, Amy pioneered the industry’s first payment dependent note that is secured pursuant to an indenture trustee and designed to be bankruptcy remote, and advised the company on its Series A funding round. In recognition her work at Patch, she was named as a finalist for the Corporate Counsel of the Year Award 2015 by LA Business Journal. Amy also brings extensive experience in legal innovation and rethinking the delivery of legal services. She is the founder and co-organizer of Legal Hackers LA, and was named one of the ten women to watch in legal technology by the ABA Journal in 2014.
The Brave New World of Robot Law

By Joel Espelien

Sensors, ubiquitous connectivity, and artificial intelligence are coming together to create a new generation of robotics. Imagine Siri with eyes, hands, and legs (or wheels). Technology is finally leaving cyberspace and coming into contact with the real world. Robots are gaining the ability to (1) sense what is happening around them, (2) plan (i.e. think about) what to do next, and (3) act upon their environment. As this sense → plan → act cycle becomes increasingly sophisticated, robots will begin to exhibit emergent and intelligent behaviors. Regardless of their consciousness (or lack thereof), intelligent robots interacting with a complex world will inevitably need to act autonomously in ways that are neither predictable nor planned by the humans that originally created them.

In other words, robot activities will increasingly come within the ambit of the law. As we shall see, robot law is neither obscure nor esoteric. On the contrary, the use of robots in our everyday lives will force lawyers to look with fresh eyes at some of the most basic principles of the law. Just as importantly, lawyers need to understand how legal developments can and will affect the development of robot technology.

As an example and a starting point, let's consider the common law of agency, which is a likely point of embarkation for robot law. The black letter legal definition of agency is a relationship created by contract or by operation of law where one party (the principal) grants authority to another party (the agent) to act on behalf of and under the control of the principal to deal with a third party. The actions of the agent with a third party bind the principal.

On first glance, agency law seems fairly well-suited to deal with human-robot relations. Imagine, for example, that my family purchases a robot nanny to help look after our three children. (If you know where I can acquire such a device please email me!) This robot is owned by me and is programmed to do my bidding. Imagine further that this robot is integrated with my self-driving car and so can chauffeur my kids to and from school, soccer practice, piano lessons, etc. Is the robot my agent for purpose of dealing with the school, other cars on the road and the piano teacher? I expect most courts will have little difficulty answering in the affirmative. The robot is my personal property and presumably acts primarily under my orders, subject only to the prime directives embedded in its code.

This conclusion initially sounds both reasonable and helpful. The school, for example, can amend its child release policies to permit children to leave campus under the care of a robot nanny acting on behalf of the child’s parent or guardian. The school is relieved of liability, I get to stay late at the office, and little Johnny makes it to soccer practice on time. Everybody wins. Viewing human-robot relations exclusively through an agency lens, however, brings with it other consequences, some of which may not be so welcome.
For example, if the robot is my agent, then the doctrine of "respondeat superior" is likely to apply. This doctrine first emerged in the English common law in the 17th century to deal with the legal consequences of masters acting via their servants. During the 19th century, this doctrine was extended from servants to employees, and became the basis of vicarious liability on the part of the employer for actions committed by the employee within the scope of employment. This became particularly important in the 20th century, when motor vehicles emerged as a new technology and the law needed to assign liability for accidents involving delivery trucks and all other manner of commercial vehicles. Respondeat superior continues to live on as a means of shifting liability to the party whom society judges as both responsible and better able (via insurance and otherwise) to shoulder liability. In the case of a robot, treating robots as employees may be problematic, but the earlier analogy to servants would seem to fit just fine. Even better, a doctrine like this lets courts "see through" the robot entirely and attach liability to the human owner. Much as courts do in cases involving dogs or other animals, vicarious liability of a human is likely to be much more legally palatable early on than direct liability of a state-of-consciousness that we don't really understand.

Many early commentators on robots may be content to end the discussion here. Ignore the robots, find the human, and let sleeping dogs lie. The innovative urges of our modern economy are not so easily quelled. On the contrary, for every legal action, there is likely to be an equally legal and opposite reaction.

For example, the law of agency and its focus on both control and the existence of the master-servant (employer-employee) relationship, gives rise to the equally important law of independent contractors. Independent contractors are not servants, but autonomous actors who are responsible for the contracted-for-service, but are free to determine the means and methods for getting the job done. In the modern context, the law of independent contractors (often referred to as 1099 contractors after the federal tax forms that are used to track non-employee compensation in the US) has resulted in the development of Uber and a host of on-demand businesses that offer services not through employees, but via an army of freelance individuals.

In the case of robots, an early and arguably overbroad application of "respondeat superior" may tend to discourage humans from owning robots directly. Why take on that liability? As in the case of Uber, other models are possible. For example, we already have a massive system for creating, empowering and managing non-human legal persons. This system is called the law of corporations and other business entities. In fact, I would submit that most business lawyers in the US today represent few, if any, humans directly. Instead, our clients are overwhelmingly corporations and other non-human entities.

These entities pay taxes, own property, have bank accounts and can freely contract for goods and services in the economy. More importantly, corporations have independent legal existence and can bring claims to the courts to enforce and defend their rights. Corporate law provides an immensely powerful conceptual tool for robots to gain legal
To wit, imagine a newly manufactured robot being contributed to a newly formed Delaware corporation. The corporation could even finance the purchase via a bank loan secured by the robot itself. The corporation has a Tax ID a bank account and a credit card. The robot then goes forth into the world and begins providing services, for example as a chauffeur for a business that provides after-school activities for kids. The business pays the robot corporation monthly for its services. The robot corporation then uses that money to rent a vehicle, pay for insurance, as well as a parking place in a "robot garage" where the robot can go when it's not working to recharge its batteries and receive any necessary maintenance. At the end of the year, the robot corporation uses a CPA and a tax lawyer file a tax return on its income. In short, robot corporations would not be mere servants, but legal "freemen" capable of living out their existence free from the ownership by, or dependence on, humans.

Although this scenario is eminently possible from a corporate law perspective, it poses serious challenges to the legal system in other respects. If a robot corporation has no human owner, there is no "easy out" vicarious liability theory for courts called upon to evaluate its actions. Imagine a car accident involving the robot chauffeur. Without respondeat superior, courts will need to assign fault between the robot and the other driver. Can a robot commit negligence? If so, what is the standard of care? Will courts have to replace the "reasonable person" standard with a "reasonable robot" standard that takes into account the unique abilities and limitations of artificial intelligences? What if the other driver is a human who becomes upset and draws a gun on the robot chauffeur (and its terrified carload of school kids)? Does a robot have the inherent right to self-defense? May a robot "stand its ground" when defending humans for which it is contractually responsible?

If a robot exceeds the scope of this right, can it be charged with a crime? Does the robot have the right to due process? If the robot corporation is unable to pay the resulting fine and declares bankruptcy, what happens to the robot? In particular, does a robot have a right to a second chance?

One quickly realizes that even basic economic liberties (i.e. the freedom to contract) lead unavoidably to the biggest questions of all. To wit, the American Revolution was fueled by a very powerful concept: "no taxation without representation." In a world where robot corporations provide our security, mow our lawns, build our houses, take care of pets, children, the sick and the elderly—and pay an increasing share of the taxes—will robots demand the right to participate in the political process (i.e. to vote)? Do free robots have a right to life (i.e. electricity), liberty (i.e. the right to not be imprisoned) or the pursuit of happiness?

The Anglo-American common law is a thousand years old, give or take, and has adapted to social evolution from manor feudalism to Bitcoin. The law will adapt to robots as well, as lawyers grapple with these issues and vigorously represent their clients, both carbon- and silicon-based.
About the Author

Joel Espelien is the founder and principal of Eseplien Law PLLC, and writes and reports on the future of media for The Diffusion Group. Follow Joel on Twitter @TheAffordableGC.
Crowdsourcing Better Access to Justice

With Mark Deuitch, by Nicholas Gaffney

Mark Deuitch is co-founder and CEO of PeopleClaim.com, an online dispute resolution service that uses peer-to-peer and crowdsourced mechanisms to resolve commercial claims. A former investment banker, Mark started PeopleClaim as a way to promote equal and universal access to justice regardless of a person's income, resources, or knowledge of law. He occasionally serves as judge at collegiate mediation contests, most recently the International Intercollegiate Mediation Tournament at Drake University School of Law. Mark is a graduate of the University of St. Andrews in Scotland, where he studied legal philosophy and metaphysics.

Nicholas Gaffney (NG): What projects or ideas have you been focusing on recently?

Mark Deuitch (MD): Our primary focus is to promote "community-based mediation" (mediation by the public) as an alternative for resolving consumer claims outside the scope of what traditional court or mediation processes can address. Our system increases public participation in claim resolution by crowdsourcing resolution ideas from our online community, and then allowing the disputants to choose the best solution to settle their case.

Another goal is to provide a more compassionate, socially responsible and time-saving way for attorneys to refer cases they can't represent. Our community-based resolution platform can provide a viable alternative for resolution of small cases that wouldn't be feasible for formal legal representation given the current costs of running a law practice. It's our understanding that 70-80% of potential plaintiffs are unable to afford lawyers to represent them.

Our goal is to help lawyers focus on their core business, while helping the country as a whole by offering a simpler yet effective alternative for the growing number of cases that can't support formal litigation. We offer a viable referral path that can also help save time when rejecting a case, especially those referred by friends and relations where the lawyer feels a need to hear details and explain their process before telling the client they're unable to help.

We're also testing public mediation in developing countries. We've partnered with a group in Pakistan to extend justice to rural villages and low-income people, and we plan other projects in the near future. Developing countries have problems that are similar to lack-of-access issues in the USA, and unique to specific cultural, political and economic situations, which our approach can help mitigate. It's likely that less than 10% of the world's population has real access to civil justice—our goal is to fix that.
NG: What could lawyers look at in a new way that would benefit their clients and society?

MD: Law has become exclusionary. By some accounts, the majority of the middle class is effectively disenfranchised from civil justice because they can't afford legal representation. This has also lead to an increase in pro se cases that further burden courts and often end badly for the self-represented. While pro bono and legal aid groups do a wonderful job helping low-income people, many don't meet the profession’s mandate to make legal assistance accessible. So, we really need to promote ways to help the middle class gain greater access to civil justice. The current trajectory is likely unsustainable, and the industry needs to address lack of access and self-representation issues.

NG: What one thing about the practice of law would you change if you could?

MD: I'd like to see law become more fairness-based and less technical. One of our goals is to promote abstract justice over technical justice through online feedback mechanisms that help the public weigh in on fairness issues. Businesses are becoming more responsive to social media opinion and we're trying to harness that movement to evolve more practical ways of resolving disputes in accord with public opinion and consumer sentiment.

There's a lot of discussion about wealth disparity. Whether wealth and income inequality is necessarily bad is open to debate, but there's no debate that a person's or businesses financial resources will have a direct impact on their success in most litigation. So the problems of unequal access to justice is being greatly magnified by wealth disparity, which is another reason we need to move beyond technical law to more fairness-based and abstract justice processes.

NG: What is the most exciting development you have seen recently in the practice of law?

MD: I like the legal insurance movement, which mirrors the medical insurance idea and allows people to pay reasonable monthly premiums to receive basic legal assistance for a wide range of needs. It can give people and businesses a backstop in case they're hit with unexpected legal issues. Just like online dispute resolution, it's offering something practical that helps address the inaccessibility problem. As with health care, law shouldn't be known for bankrupting families just because they have a problem that requires professional legal expertise and assistance.

NG: What technologies, business models, and trends do you think will have the biggest impact on the practice of law over the next two years?

MD: A while back, "legal tech" was a popular theme in Silicon Valley. Unfortunately, a great deal of money invested has been written down—not an uncommon thing in the first wave of any investment fad. Applications, including Big Data, that allow lawyers to be more efficient, project outcomes better, and
help match clients with attorneys are still exciting and might even reduce the cost of pursuing justice. I personally like sites like Avvo and Quora, which can help laymen get answers to questions about law and other matters from a wide range of experts and practitioners.

We're doing some early-stage work to determine if an algorithm could actually win a case or handicap a case and its outcome probabilities. But this is all early-stage. We don't think lawyers have to worry about being replaced by computers in compound litigation any time soon. What's clear, however, is that if a process can be automated, offshored, or otherwise simplified, it will be, and legal practitioners need to move away from "commodity" to higher-value services if they intend to maintain current revenue standards.

NG: What's the best new law practice idea you have heard recently?
MD: Several of the ideas I've noticed in previous "New Law" interviews are intriguing. I've mentioned legal insurance as a promising approach. The "low-profit firm" idea obviously could fill a need.

As an entrepreneur, I like Reg A and other developments that allow start-ups to raise money through crowdsourcing and online mechanisms. Those will need to be watched for abuse and the vulnerability of less-sophisticated investors making big mistakes, but in theory the concept is great. The legal industry can and should play a big role in facilitating this new freedom. I'd advise anyone seeking funds and, more importantly, anyone providing funds, to hire experienced counsel before making a big commitment.

Also, as mentioned, PeopleClaim is creating a referral network for cases lawyers have to turn away. The legal profession either needs to fully serve the needs of the populace—especially middle income groups—or offer viable alternatives beyond pro bono or legal aid. In our view, a democracy where a large portion of the population is disenfranchised from civil justice isn't sustainable.

Note: The other co-founder of PeopleClaim was the late Carl Singer, former CEO of Timberland, BVD, Scripto, and Sealy.
The Future Is In Our Hands: Biometric Identification As Authentication

By Marcello Antonucci and John P. Morgan

Would you dig a moat to protect your house from burglars? Of course not. Why, then, do we use similarly archaic means like the alphanumeric identifier and the password to protect our electronic data?

Change is coming, however. A number of intrepid companies are now making use of technological advances in biometric identification—unique physical attributes such as fingerprints, facial structure and iris scans—as an alternative or added layer of authentication and fraud prevention. While public sentiment surrounding the use of biometric identification as a means of security authentication appears to be shifting from stark skepticism to cautious acceptance, companies need to be aware of the privacy concerns and new potential theories of liability they will face when establishing biometric identification programs.

Given the limited use of such programs in the United States to date, it is instructive to look to India, where the Unique Identification Authority of India (UIDAI) is home to the largest biometric identification program ever assembled, with biometric information for more than 940 million individuals. India’s foray into biometric identification began in 2009 with the creation of UIDAI, whose goal is to provide every Indian resident with a biometrically-secured form of identification known as "Aadhaar." UIDAI collects fingerprint, iris and demographic data, along with a photograph for each applicant, and correlates that information with a twelve-digit identification number that can be used as universal proof of identity for a range of public or private services, from obtaining social assistance funds to opening a bank account. Each applicant’s information is stored in a centralized database that allows for real-time biometric authentication in the event an Aadhaar number requires confirmation.

As the project progresses, it promises to provide all Indian residents with digital, easily verifiable and—most importantly—universal identification. Identification is especially valuable to India's lower-income population, most of whom do not have other reliable means to confirm their identities which could delay and/or preclude access to government assistance programs and prevent use of private sector services such as banking.

As promising and ambitious as the Aadhaar project is, questions regarding individuals' privacy rights and security of the information provided to UIDAI loom large over the project. UIDAI's critics raise concerns about the potential for misuse of enrollee's biometric information, as well as the inevitable threats of hacking and data theft. With so many accounts and services tied to a single unique identifier, Aadhaar may unintentionally serve as a gateway to increased state surveillance.
In addition, the sensitivity of the biometric information and centralized Aadhaar database mean Aadhaar could become a prime target for hackers and identity thieves. The July 2015 breach affecting the United States Office of Personnel Management, which resulted in the suspected theft of 5.6 million government workers’ fingerprints, shows how attractive such information can be despite limited present value in the United States.

Biometric identification's greatest strength also has the potential to be its greatest weakness. While intrinsic physiological characteristics—like fingerprints and iris scans—are unique and more difficult to forge than a username and password combination, these same traits can make biometric information difficult to replace in the event of theft. Obviously, an eye or a fingerprint cannot be replaced as easily as a password. In order to achieve long-term viability, UIDAI will need to ensure that the biometric information it collects is subject to strict information security protocols in order to minimize the risk of unauthorized access.

Yet despite the unique, sensitive nature of biometric information and vast scope of the program, India has not yet passed comprehensive privacy legislation governing the protection and permitted use of data collected in connection with the Aadhaar program. Similarly, there are limited regulations governing the protection and use of biometric information in the United States. As of January 1, 2016, there are only seven states (Connecticut, Iowa, Nebraska, North Carolina, Oregon, Wisconsin, and Wyoming) that consider biometric information to be "personally identifiable information" that would trigger a private entity's notification obligation in the event of a breach, three of which enacted legislation to expand the definition to include biometric information just this year. Accordingly, there could be a breach of highly sensitive, unique biometric information, but a company would have no legal obligation to notify the individual that their information had been compromised.

Furthermore, there are currently only two states (Texas and Illinois) with laws specifically regulating the collection and use of biometric information by private companies outside the education industry. The Illinois Biometric Information Privacy Act, 740 ILCS 14 et seq. (BIPA) provides that a private entity must notify an individual and obtain consent to collect, capture, purchase, or otherwise obtain a person's biometric identifier or biometric information. BIPA also prohibits the sale, lease, trade or profiting from a person's biometric identifier or biometric information, without exception, and requires that a business in possession of biometric data develop a written policy concerning biometric data retention and deletion. BIPA provides a private right of action, and recovery of liquidated damages in the amount of $1,000 per negligent violation, and $5,000 per intentional or reckless violation of BIPA.

Meanwhile, the Texas Business and Commercial Code Annotated, §503.001, Texas' biometric protection law, contains some of the same protections as BIPA, but does not contain the same requirements that notice and consent need to be in writing, nor does it require the disclosure of the reasons for collecting biometric information and how long
the information will be stored. The Texas Code also provides that a party may sell, lease or disclose biometric identifiers in certain limited circumstances. The Texas Code provides a penalty cap of $25,000 per violation, and permits the Texas Attorney General to bring a civil action to collect that penalty rather than a private right of action.

With liquidated damages per violation, BIPA has become a popular tool over the last year for consumer class action attorneys. Facebook, Shutterfly, Google, and Snapchat have all been sued in Illinois for alleged violations of BIPA for the purported unauthorized creation, collection, and storage of users' facial geometry, a form of biometric information, without consent. Additional actions are likely to follow as more companies—like MasterCard and Deutsche Bank, two companies that have recently announced they are (or are considering) implementing biometric identification programs—enter this domain.

As individual states begin to adopt standards concerning the use and disclosure of biometric information, companies that maintain biometric identification programs will need to keep up with the changing regulatory landscape in much the same way that companies have navigated evolving privacy and breach notification standards over the last twelve years. At the same time, legislation requiring the protection of biometric information and dictating the permitted uses of that information could lead to increased use of biometric identification programs. Companies would have clear guidelines to follow when implementing biometric identification programs, and consumers would know how their information was being used and protected, instilling greater confidence in providing such information for use in such programs. Lastly, companies should seize the opportunity to partner with government and global experts in privacy law and risk management to become leaders in in the adoption of biometric identification.

About the Authors

Marcello Antonucci is a claims manager for technology, media and business services at Beazley Group, and is experienced in privacy and data security. John P. Morgan is an attorney with Clyde & Co., focusing on data privacy and security.
The Internet of Things: Ubiquitous Legal Issues

By Immanuel Kim

Detective John Andersen, in Minority Report (2002), was standing before the virtual dashboard utilizing the multi-touch interface to analyze 3D pre-crime data to enforce the law. Afterwards, as a fugitive, John was suspensefully recognized by advertising screens calling his name and making offers. That is one example of a convergence of Augmented Reality (AR) technologies and the Internet of things. The 3D data is now called as "big data." Those products are already available in the market; so that movie is not entirely fictional. According to FTC's 2015 Internet of Things Report, the Internet of Things (the "IoT") is defined as: "the ability of everyday objects to connect to the Internet and to send and receive data." No surprise, all industrial roads lead to the Internet of Things. Very true. For that reason, some experts may deem the IoT as infrastructure for "Industry 4.0." That movement comprises and completes the cyber-physical interaction adding up to prior mechanization, electronization and automation. That novel, beautiful automation is even intelligent. In 2015, the number of the Things was estimated at approximately 15 billion across the globe; it will take only five years to reach 30-50 billion devices, according to common estimates. Although some depictions are under development, our today is very close to such ever-dreaming fantastic society.

The Things: Lawyers' Technological Enigma

Legal issues orbiting technologies are more convoluted than those technologies. There is no compelling reason to discuss the IoT distinctively from artificial intelligence, robotics, drones, cloud computing, mobile computing, big data, virtual reality, manufacturing automation and even consumer electronics. The main reason is that the IoT is the technological subconsciousness of all future technologies; the industry is interested in the humongous data traffic through the devices that are all inter-connected, also linked to the cloud or dedicated storage. In this context, future products and services will be all aligned along a smorgasbord of emerging technologies. Abundant smart products are already coming into play. "Every effort to reduce a case to a rule is an effort of jurisprudence." Look at legal matters on the Internet of Things as a bad man, as Oliver Wendell Holmes once remarked. Our predictive jurisprudence may extend to address the benefits and risks of an authentic 'disruptive innovation.'

Legal approaches become efficient when the IoT phenomena are analyzed and articulated on three levels or terms: Device, Network and Data. Whether the matter is related to either industrial IoT or consumer IoT, this IoT equation helps not dawdle in the course of technological and legal development. Aside from possible noise, legal issues arising from the IoT confusion may encapsulate into this equation: The FTC Staff Comment on the IoT, on June 2, 2016, made a broader leap from the 2015 Report's viewpoints to embrace more network and data issues orbiting the IoT development, more significantly discussing interoperability and big data matters.
The Internet of Things as Device

The Things are now incorporated into every facet of our lives: smart homes, wearable devices, smart cities, smart grids, industrial internet, connected cars, connected health devices, and smart retails. The most innovative part of products and services through the IoT devices is automation. Businesses anticipate rampant automation of their processes and productions, achieving historically the highest productivity. Lawyers think that the key nugget of automation may be 'automated decision making' where programming codes provide data-driven decisions, self-learning, and self-modifying via internal and external interactions.

Contractual issues arising out of the IoT devices may not even novel to us. From Vending machine through e-commerce to blockchain, examples already abound around us. In this regard, the buyer-seller interfaces may be diversified as the Smart Things are prevalent in the market. Take smart contracts, credited to Nick Szabo in the 1990s. The concept of smart contracts has been taking shape along the recent digital revolution. Although the concept is organic, its essence may be executable computer codes wholly or partially replacing traditional terms and conditions of contracts not to mention the mutual assents. The beginning of such technology was certain automation purposes to avoid infinite repetition of the same type of jobs. At the advent of online trading, our first automated contract has been, at best, in the form of 'Click OK,' or 'I Agree,' ensued by electronic signature. Prior to the Internet Age, vending machines had embedded codes to implement certain automated contracts although the level of communication is elementary. Contemporary advance in automation is algorithmic trading. The algorithmic trading, in the stock market, is a computerized process to apply a certain set of rules including price, quantity, and timing in order to place a trade faster than human traders can.

A leap forward in automation, the functions of computer codes will extend, to a certain degree, to interpret the facts and apply rules, which is supported by big data and its analytic techniques. The smart contracts could be formed between intelligent machines, which is useful in supply chains. One advanced commercial example is the trustless public ledger (TPL), a system underlying the Bitcoin cryptocurrency. Imagine John Andersen, while he was being chased, purchased a new cell phone or a water bottle from advertising screens or other IoT devices. John would follow a certain steps of smart contracts; no customer representative would work with John. In the same line of thought, the EU's new regulatory trends on data breach will include disclosure of underlying logic or algorithm employed on the analytics and software platforms, which is first effective in 2018. Now we know why.

The other drawback of the IoT may be injuries arising from the physical devices. Tort claims may be based on either negligence or product liability. In the near future, our public and personal space will be filled with smart home devices, wearables, unmanned cars, and flying drones. Humans in this IoT sphere are all vulnerable to injuries due to malfunction of devices where devices fail to work normally due to manufacturing failure, hacking, malicious codes, or even electromagnetic interference. This year, several crash cases on smart vehicles and drones have been reported. Despite the continuous improvement, the inherent risks in physical objects, either flying, speeding, or heating, may be doomed to cause certain harms to humans or properties. There is an urgent need to set up minimum security and control
requirements for IoT devices. The precautions may be attained by certain design
requirements, not by post-accident management.

The Internet of Things as Network

The smart devices are connected through certain networks: LAN, Wireless (LTE), Bluetooth,
Wi-Fi, Radio-frequency identification (RFID), you name it. Aiming at the maximum utilization
of heterogeneous devices and protocols, interoperability must be ensured within a
constellation of electronic pieces. In 2016, the first battle for the IoT standardization has
ended, ready for deployment at the end of the year. The 3rd Generation Partnership Project
(3GPP), in June 2016, has released new standards of Narrow-Band IoT (NB-IoT), enabling
low cost, low data rate, and longer battery life for the IoT devices. Along with eMTC
(enhanced Machine Type Communications), covering medium data rate, the NB-IoT supports
indoor use where cellular and Wi-fi do not function well. NB-IoT equipments are already
developed and tested, about to hit the market by 2017. Also, oneM2M, a new global standard
for machine-to-machine (M2M) communication, was released and updated in March 2016.
The specifications of the standards cover HTTP, CoAP and MQTT, common industry IoT
protocols. Furthermore, in July 2016, the Federal Communications Commission (FCC)
opened more spectrum for the IoT uses. Meanwhile, the wireless industry has completed
technical specifications and significant testings for the next generation wireless technology
5G. Target Wonderland in New York City is exploring the maximum utility of RFID technology
in retail services. In 2018, 3GPP may announce another gift, 5G New Radio covering the air
interface for drones and other flying objects. Therefore, our Connected Wonderland comes
near us as the interoperability has been rapidly elevated.

The Internet of Things as Data

The FTC Staff Comment on the IoT highlights the importance of the data by defining that the
IoT implies "the ability of everyday objects to connect to the Internet to send and receive
data." Big data is the most valuable when it creates deep business insights, better in real
time. By sharpening such insights, the business can improve their management, customer
services and handle risk factors, which are also beneficial to consumers. Big data analytics
plays a central role in the IoT applications across the IoT constellation. All kinds of data and
metadata are latent in the connected electronic pieces and the data proliferates across the
networks, storage and devices.

For example, traditional insurance premiums are determined by various factors including
medical prices, benefit cost, geography, demographics, member changes, benefit design,
regulations and administration. The IoT enables usage based insurance (UBI) to leverage the
premiums based on big data collected from the beneficiary's environment. Odometer and
GPS data have already in active use for premium determinations. More data may be available
from the Things deployed in smart homes, smart cities, connected health devices and
connected cars. Furthermore, insurance companies, by utilizing personalized data on
customers, can extend their services to emergency assistance, vehicle tracking and other
value added services. This is another aspect of the IoT revolution.
Data breach is a flip side of the coin named big data. The *FTC Staff Comment* pinpoints the potential security risks residing in the Smart Things as: "(1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks." Security and data breach may be the most imminent legal issues before us. In the old Internet regime, security concerns and certain tools are present at each level of the Internet structure. Nevertheless, the current level of mobile security is extremely low. Even worse, security tools for the IoT are under development and, in fact, open to various intrusions. Bernard Marr estimated in *Forbes, April 1, 2016*, that an annual increase in data production will be 4300% by 2020. Massive data collection across the Things poses a manifest threat to the users' privacy. Two of the FTC's recent cases clearly showcase the formulation of a new regulatory framework on the IoT environment: *In the Matter of ASUSTeK Computer Inc.* (2016) and *In the Matter of LabMD, Inc.* (2016). Through the two post-TrendNet cases, the FTC has envisioned a blueprint for its regulatory guidelines. ASUSTeK Computer Inc. is a Taiwanese corporation, the second largest router manufacturer in the U.S. router market. In 2014, its routers had a vulnerable security settings allowing 12,900 personal data to public availability; nevertheless, the electronics' advertisement made promises about the high-level security to consumers. The case was settled by admitting comprehensive security program.

Especially, the *LabMD* case exhibited the pivotal requirements to determine the fair practice for the IoT business although the decision is not final. LabMD, Inc. is a clinical testing laboratory, based in Sacramento, CA. In 2008, the company's spreadsheet containing insurance billing information was found on a peer-to-peer network. The spreadsheet contained more than 9,000 consumers' personal information. In addition to that unauthorized exposure of consumers' personal data at risk, the laboratory was also found, in 2012, to let certain documents in the possession of identify thieves, including sensitive personal information. While ordering comprehensive information security program to the company, the *LabMD* decision includes that: (1) the "reasonable design" of comprehensive information security program; and (2) the "full documentation" of such program's contents and implementation are the key parts of fair security practice possibly enforced by the FTC. Overall, the FTC's regulatory guidelines under the "unfair business practice" provision (*Section 5 of the FTC Act*) are zeroing in on comprehensive security measures, advertisements, and independent auditing.

**Legal Dynamics: A Logical Leap to Solutions**

The Internet of Things has been evolving from high-end electronics, advanced information technology, and enormous data mining techniques. The Things, despite potential benefits on even low-income and underserved populations, still bears the same issues such as net neutrality and the IoT divide. In this regard, Jeremy Rifkin's excerpt in *The Huffington Post, April 7, 2014* is insightful when he contrast monopoly capitalism and collaborative commons. With all the various ramifications and implications of the Connected Wonderland, the future of the IoT is still obscure. Learn from the Betamax vs. VHS format war at this incubating stage. Technological idealism does not survive in the modern world. Despite numerous tech roadshows, the society is yet to realize its true potential. The real picture depends on: Which
technological options would dominate the market through regulatory labyrinth and consumer choices; then more specific policies can ensue. "Connect your subject with the universe" of the IoT and catch "a hint of the universal law." Good luck.

**About the Author**

**Immanuel Kim** is a New York bar candidate, interested in technology law and legal technology, bioinformatics, artificial intelligence, big data analytics, and e-discovery.
Weary of Wearables: IP, Privacy, and Data Security Concerns

By Zainab Hussain

Have wearables signaled a new focus on couture from Cupertino? It's on the rise, but not just yet. Not when the relationship everyone thought would be steady by now is firmly in the "It's Complicated" phase.

The fashion and technology industries have certainly recognized a gap in the market where they intersect, both in terms of fulfilling societal needs (needs we never even knew we had), as well as in lost revenue streams. Sales of wearables amounted to roughly $3.5 billion in 2014, and due to improving data reliability and product variety, industry experts expect sales to increase five-fold in the next five years. This is occurring in the face of whole groups, such as the Chinese People's Liberation Army, banning the use of certain wearables by soldiers, for fear of increased trackability and a higher chance of leaking military secrets.

As the wearable technology industry grows, the legal community must address the new and inevitable intellectual property concerns that manufacturers and technology companies will have, as well as consumer data security and privacy concerns associated with FitBits, Fuelbands, and other wearables. Makers of wearables must protect their IP in innovative ways; as technology companies and fashion houses partner, who owns what is a growing concern. Consumers are weary about the security of sensitive personal data and have concerns over their ownership of such information. Lawyers need to understand both the technology and the business behind it to counsel clients most effectively.

Part of the rising success of wearables, despite their inherent privacy risks, is their "coolness" factor. One way manufacturers of wearables have sought to achieve positive consumer connection is by associating with fashion houses and designers who have mass-market appeal. Apple made some strategic hires, enlisting executives at Burberry and Saint Laurent to assist with designing the Apple Watch. Google Glass co-brands with Diane von Furstenberg (the Queen of Cool), and Ray-Ban.

Through these partnerships, attorneys have been careful to address intellectual property ownership by dividing the assets into two vague camps—the IP that stems from the technology, and the IP residing in the brand value. Trademarks must be safeguarded and used correctly in marketing and branding the wearables. Attorneys must be able to quantify their clients' brand values in dollar amounts as compared to the companies they partner with. In addition to trademarks, wearables are one of the few technology consumer products that garner value in trade dress. Among others, Nike has capitalized on the Fuelband's distinctive and readily recognized shape and design, so
as to create trade dress protection around the device. It will be interesting to see how attorneys deal with features of wearables that blend design and technological function, as trade dress remains a historically underutilized form of IP protection.

As is often the case, however, patents offer the greatest protection for wearable technology, and unlike many other patentable innovations, wearables offer manufacturers the opportunity to invest in both utility and design patents.

Patent investment and enforcement can also lead to the most costly of legal battles. An upgrade in the form of a wearable installed in Ralph Lauren's signature Ricky bag is the subject of an ongoing patent infringement lawsuit. The handbag features an illuminable interior, and a charger for electrical devices. An inventor claims this technology infringes on his utility patents for an "electric accessory system." Also named in the suit is Leoth Inc., the technology partner that Ralph Lauren worked with to produce the $5,000 luxury handbag, and Kickstarter Inc., where Leoth's light-up-juice-up technology was initially sold. It remains to be seen how this case plays out, and, if in fact infringement is affirmed, how damages are accounted for between Ralph Lauren Retail, Leoth, and Kickstarter.

Adidas and its technology partner, body sensor manufacturer Textronics, are embroiled in a patent infringement lawsuit filed by a different body sensor products manufacturer by the name of Sarvint, over the use of sensor technology employed in Adidas' line of miCoach training shirts. The shirt uses special fibers to measure the wearer's vital signs, and is linked to a smartphone app.

The fact that utility patents are spilling over into the fashion industry—an industry that from an IP perspective previously was focused on design rather than technological innovation—and across several devices at once, may be cause for patent litigators to pay closer attention to an industry often considered frothy and frivolous.

The IP issues faced by wearables manufacturers and technology developers are largely familiar, and previously addressed in different boom industries at various times. But wearables also bring issues of privacy and data security that may be novel to many attorneys. The largest regulatory voids exist in these two areas of law, and the legal community must highlight and educate on risks of data loss or theft, and privacy violations, as well as demand a more concrete framework to address these concerns.

Data protection is a key consideration for manufacturers of wearables, and those developing for wearable devices. The security of data collected from users of wearables, especially data considered "personal information" (such as health, financial, and location data) is important, because through personal information, it is possible to identify the individual to whom the data is linked, either by a single piece of information or by triangulation and combination of information. Unauthorized, unintentional or overreaching use and dissemination of personal
information creates potential liability for several parties.

Consider this: Jo wears a device that collects information through an app about her blood pressure, heart rate and the number of steps she takes in a day. The device manufacturer gathers and stores the data, all tied to Jo's account, which she was required to create to use the app on her wearable device. The manufacturer of the device or app developer could use the information to present Jo with targeted, strategic advertising. Since Jo's been taking over 15,000 steps a day, on average, perhaps she's in the market for a new pair of sneakers? This kind of data use falls on the more innocuous side of the spectrum, because it is the wearer's data being boomeranged back to the wearer herself, in the form of advertising.

However, data security concerns of the more nefarious kind are at play when the wearer's data is disclosed—intentionally or in error—to third parties that can have huge impacts on the wearer's quality of life. Data sold, stolen or leaked through a data breach, to third parties such as insurance providers, for example, could allow insurers to quote Jo higher rates for health insurance, or even cancel her policy, without her knowing how or why, or even that the insurer was able to access her wearable device data.

The risk of breach is so tangible that many companies are purchasing cyberinsurance, to protect themselves from the liability arising out of a data breach. Although not directly a breach resulting from wearable devices, Columbia Casualty v. Cottage Health System, No. 2:15-cv-03432 (C.D. Cal., 2015), highlights the important issues and value of health data breaches, the type of data collected by the most popular wearables.

In that case, private health data belonging to some 32,500 patients, stored on network servers owned, operated and maintained by Cottage Health, was negligently disclosed in the public domain via the Internet. That case settled with Cottage Health's insurer, Columbia Casualty, shelling out just over $4 million. Columbia Casualty sought to recoup the settlement amount, based on two claims. First, Columbia Casualty alleged that Cottage Health failed to "continuously implement" minimum security practices, and to "regularly check and maintain security patches on its systems". Columbia Casualty's second claim related to the misrepresentation of material facts regarding Cottage Health's maintenance of risk (of breach) controls.

Although currently in mediation, the peremptory case highlights the work that successful attorneys counseling in the areas of data security and privacy law must do. It appears that preventative measures are better than an entirely curative approach to dealing with liability and risk of privacy violations and data security breaches. Lawyers may draft the most airtight and overreaching privacy policies and end-user license agreements (EULAs) for their wearables manufacturer or technology-developing clients, explicitly informing wearable
users that their data can and will be used. At the end of the day, however, it is unlikely that these agreements would be held to be enforceable.

A better practice would be for attorneys to counsel their manufacturer and data controller clients on limitations of data use, and the risks of data breaches. Attorneys must be able to advise on the adequate levels of security and protocols required to withstand scrutiny in light of current industry practices and forecasted risks of data breach and privacy violations. Health and financial data are more risky than certain other types of personal information because they are more sought after. And in light of Columbia Casualty, attorneys should attempt to negotiate cybersecurity insurance policies on behalf of clients, to reduce the likelihood of an insurer successfully avoiding or limiting coverage in the event of a claim.

Privacy regulations need to be put in place and be enforced before, for example, blood pressure information collected during rush hour gets sent to your auto insurer, causing you to be classified as an aggressive driver. In the U.S., the FTC enforces consumer protection and consumer privacy rights where companies mislead, or fail to maintain adequate security for sensitive consumer personal information, under Section 5 of the FTC Act (barring unfair and deceptive acts and practices in or affecting commerce). The most recent example of privacy breaches comes in the form of a settlement between the FTC and Wyndham Hotels and Resorts, after Wyndham was found to have "unfairly exposed credit card information of hundreds of thousands of consumers to hackers," in not one, not two, but three data breaches. Under the settlement, which places Wyndham under obligation for 20 years, Wyndham must adhere to strict auditing and security certification procedures.

Attorneys can learn from Wyndham's mistakes, to be better able to counsel clients on managing data breaches, whether the clients are individual users or manufacturers of wearable technology and devices.

Once again, a preventative approach would have saved Wyndham much public scrutiny, skepticism and some serious cash. Attorneys need to be able to converse with the technical experts that handle their clients' data, and who put in place the various levels of encryption and other security protocols, in order to meaningfully assess the clients’ exposure and areas of risk and liability. Preparing EULAs, privacy policies and going about generally counseling clients who develop for or directly manufacture wearables will require attorneys to be educated on the capabilities of the devices, how data is accessed, managed, disseminated and protected.

Until regulations that speak directly to the collection and dissemination of data through wearables—arguably all of which is personal information—are put forth, attorneys must keep abreast of case-by-case updates on the types of breaches that are occurring, and make sure that clients are protected, at minimum, against known threats.
The other side of privacy concerns associated with wearables is third-party contact with a user of a wearable device. Certain wearables, like Google Glass, may intrude on the privacy rights of others who may not consent to being filmed, recorded or otherwise included in the wearer's information collection activities.

The law has not yet addressed several concerns for third parties here, but it is important to be cognizant that such issues exist. Who owns the data that ropes a third party who did not consent to being recorded? What rights does that third party have in demanding a copy of the data, or in demanding deletion of the data?

As devices get smaller and more inconspicuous (some smartwatches are intentionally designed to look identical to their traditional timekeeping counterparts) how do we account for the presence of wearables in settings where proprietary and confidential information is being disclosed discreetly, especially if we don't even know they're there? And ultimately, who bears the responsibility and liability for unauthorized dissemination of the data—the data collector who took all the reasonable security measures, or the wearable-wearing thief?

Industry experts conclude that by 2025, more data will be generated from sensors and wearable devices than all of the data being generated today from any other source. This makes sense: wearables, by definition, are small and portable, meant to be worn and taken with you wherever you go, during your waking and sleeping hours. Wearables are meant to be real time, 24/7 personal trackers of your mood, shopping needs, caloric intake, heart rate, proximity to destination... the list is endless.

As of now, we have not seen headline-grabbing data breaches involving data collected from wearables, which more often than not, measure health and wellness indicators, from check-ins at the gym to number of hours slept. Additionally, the wearables market is too nascent to have encountered its share of patent infringement mega suits. This may be why so little has been done by the legal community and policymakers to address the risks, and how to deal with them.

As with all technology, breaches and subsequent legal action are only a matter of time. The difference with wearables is that the value of health and wellness data has proven to be more valuable than stolen credit card numbers. After all, bank accounts can retroactively be corrected for fraud, but the health information of a wearable device user is inextricably tied to that user (in many ways, the data is simply a slice of the pie that makes up the person). In the absence of solid regulations, we need to be aware of the legal implications of introducing an increasing number of wearables into our everyday lives, and understand the technology behind the wearables and how it is used, in order to effectively counsel clients. The legal community—both in private practice and in public policy—can be the first point at which public concerns over privacy of data are
addressed, by pushing all the actors in the wearables industry to expend greater efforts to ensure data security.

**About the Author**

**Zainab Hussain** is an attorney with Foundry Law Group in Seattle, and focuses her practice on intellectual property issues. Follow Zainab on LinkedIn.
The Resurgence and Relevance of Bitcoin: What You Need to Know, and Why

By Benjamin Katz

In January 2015, one Bitcoin was worth $177.28. As of mid-December, the currency is worth $463.67. Bitcoin is experiencing a resurgence, and it may now be worthwhile to spend some time learning about the virtual currency.

It is likely that less than 1% of all attorneys understand how Bitcoin, and the blockchain technology underpinning the cryptocurrency, really work. That is not due to the collective ineptitude of the bar, but the immense complexity and cutting edge nature of the subject matter.

This is not necessarily an issue of importance to lawyers, as cryptocurrencies are not likely to have an immediate impact on most law practices. Clients are not going to start paying bills in Bitcoin, and if they did, a cursory Google search would provide instructions on how to cash out.

Below is a brief explanation of Bitcoin, and how it might impact the legal industry.

Bitcoin is a decentralized virtual currency. The U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) defines virtual currencies as

"a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. A convertible virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency. In other words, it is a virtual currency that can be exchanged for real currency."

Bitcoin is a convertible virtual currency that is not issued or regulated by a central government or authority. Instead, transactions of Bitcoin are collectively verified by a peer-to-peer network, called the blockchain. This is where things get complicated.

The vast majority of legislators, like attorneys, do not have an understanding of the fundamental principles at work behind cryptocurrencies. This has led to a void of regulations that are focused on issues that arise out of the use of cryptocurrencies.

To date, the word "blockchain" is absent from all federal and state statutes. Bitcoin is mentioned only once, in a California statute that criminalizes the sale of raffle tickets in exchange for "Bitcoin or any other cryptocurrency." Cal. Penal Code § 320.6.

In 2014, the state legislature of Oklahoma added an official comment to a statute to
address the transfer of Bitcoin, and its impact on secured transactions. Okla. Stat. Ann. § 1-9-332 states that a transferee of money, or of funds from a deposit account, takes the money or funds free of a security interest, unless the transferee acts in collusion with the debtor in violation of the rights of the secured party.

The official comment to Okla. Stat. Ann. § 1-9-332 now states:

"As of 2015, the use of so called "bitcoins" and the like have gained traction as a form of "currency," i.e., as a payment method. Some sellers of goods or services are willing and able to accept bitcoins in payment. If that payment instead were made in cash, or by a check or other transfer out of a deposit account, any security interest in that, e.g., as proceeds of the deposit account based on the claim of a secured party that has a security interest in inventory, would not impair the payment to the seller or other transfers to a third party. See section 1-9-332 and section 1-9-315(a)(2), (c) and (d). This is a consistent policy under UCC Article 9 -- see, for example, sections 1-9-320 and section 1-9-321, and is particularly strong with respect to 'currency.' However, section 1-9-332 cannot be construed to protect the receiver of bitcoins."

Interestingly, the Oklahoma legislature has determined that a seller who accepts Bitcoin does not take the cryptocurrency free of an existing security interest. It is unclear what policy supports this distinction under Oklahoma law.

Bitcoin and the blockchain's absence from federal and state statutes does not mean that it is outside the purview of legislation passed prior to the launch of Bitcoin in 2009. FinCEN has designated virtual currency exchanges and administrators as money transmitters, subject to an array of federal and state regulation.

Furthermore, state regulatory agencies have promulgated rules that impact businesses involved with cryptocurrencies. Recently, the North Carolina Commissioner of Banks has taken steps to make the state an attractive place for virtual currency businesses to open up shop, including exemptions from certain licensing requirements.

The New York Department of Financial Services, on the other hand, has recently launched a "BitLicense" plan, which requires virtual currency businesses to apply for a license, which comes with a $5,000 price tag. The New York rules are lengthy, and the impact on virtual currency businesses is yet to be determined, but one provision is clear: if your application is denied, the $5,000 application fee will not be refunded.

The National Conference of Commissioners of Uniform State Laws has published a draft of the Regulation of Virtual Currencies Act, with the goal of harmonizing state laws regulating virtual currencies. Such regulation aims to both protect consumers and encourage innovation.

Whether or not the uniform act will gain traction is unclear, but the future of Bitcoin seems bright.
About the Author

Benjamin Katz is an associate in the Nashville office of Frost Brown Todd, LLC. Ben primarily works on complex cases involving business disputes for an array of clients, including clients in the payments industry.
Integrative Law: 
Evolution of the Legal System

By J. Kim Wright

By the time I graduated from law school in 1989, I had decided that I never wanted to be a lawyer. I'd gone to law school with high hopes for making social change and helping people; interactions with my classmates and the legal system had dashed those hopes. I worked in the nonprofit world for a few years, running a domestic violence agency and working in an organization dedicated to ending hunger.

In November 1993, I was in a personal transformation course when a tall, distinguished man stood up to introduce himself. His presence got my attention. His words transformed my life. Forrest Bayard was a divorce lawyer, and he shared his philosophy of practicing holistically, as a healer, granting dignity to everyone in the process. As a family lawyer, his goal was to help clients end their marriages and still be amicable co-parents. That brief introduction opened a new possibility for law and me. I wasted no time. By March 1994, I was a member of the North Carolina Bar.

I opened my office and soon found that a lot of what I had feared about being a lawyer was actually true: many colleagues were argumentative and seemed to enjoy inflaming and escalating conflict. Litigation was often harmful to already precarious parenting relationships. But, for me, something was different. I now knew that it was possible to practice law in a different way.

I began to design my law practice based on my own values and aspirations. As a self-identified holistic lawyer, I sought out the most innovative peacemaking and healing approaches to law. Over the course of the next 14 years, I became a mediator, a collaborative lawyer, a restorative justice practitioner, a lawyer-coach, and more. I learned plain language drafting and began to write relationship-focused contracts. I became involved in humanizing legal education, therapeutic jurisprudence, and creative problem-solving. I studied neuroscience, appreciative inquiry, systems change, and non-violent and non-defensive communication. I worked on my personal transformation and looked for ways to integrate that in my law practice. My clients responded enthusiastically.

I began to meet other lawyers who were on similar paths. I was not alone! In 2007, I was involved in more than a dozen conferences as an organizer, speaker, and attendee: holistic law, humanizing legal education, collaborative law, Lawyers as Peacemakers, ACR, etc. The conferences were hosted by diverse groups, but the themes were similar, and the content was holistic and innovative. My study of systems change had helped me to see that movements are created by innovators who connect with each other, share ideas, and gain courage from knowing they are not alone. I saw
an opportunity to make a difference as a connector.

Early in 2008, I began an adventure of traveling around the world, finding, supporting, and connecting innovative lawyers, while chronicling this fledgling movement. I expected to be gone for a few months. I am now nearing the end of my eighth year as a nomad. I have spoken with and to thousands of lawyers, law students, and others involved in law and conflict resolution. I've been to five continents and many countries, with plans to visit the last continent (South America) in 2016. Just as I saw the seeds of a movement in 2007, I've seen the same evolution among different practice areas, and across disciplines, in every country where I have visited.

What I've observed has been an evolution of law that reflects the evolution of society, although admittedly, our profession doesn't change as fast as others. That is partly by design: law is based on precedent. It provides stability for society and keeps us from just jumping on fads. The existing system was built on the societal values of the past. Integrative lawyers are creating models and approaches based on the current societal values. They are experimenting, innovating, and piloting new models.

When I talk about Integrative Law, I often talk about some of those emerging models. Perhaps someone has heard of restorative justice through the frequent press coverage in the New York Times and episodes of Oprah. Maybe they've heard of Wevorce, the amicable divorce technology model which has appeared in the Wall Street Journal, Forbes, and many other publications. For some, mediation or collaborative practice are familiar. Sharing law is intriguing. In-house counsel resonate with Conscious Contracts. Our conversations start with something familiar, like the need for clarity in contracts, and then we step back and discuss innovations.

Over the years, in country after country, I've heard the same story over and over—and my own journey is pretty much the same as those I've heard. Becoming an integrative lawyer is an evolution with a predictable pathway. Not everyone takes the journey, not everyone takes every step, and sometimes the order varies, but there is enough of a pattern to see the trend. Perhaps you will see yourself on this path.

Responding to the Tripartite Crisis: Something is wrong here!

First, lawyers experience some aspect of what law professor Susan Daicoff calls a "tripartite crisis" in the legal profession: low levels of lawyer well-being, low public reputation, and incivility among professionals. Statistics show that for many, our profession has high levels of depression, addiction, relationship dysfunction, and suicide as compared to the general public. Most of the integrative lawyers have hit the wall in some way and begin to look for a better way.

Of course, some lawyers enjoy their work and think their lives are just fine. Those
lawyers tend to see that something else is possible, that they can enjoy their work even more.

Reflecting on self, relationships, and the profession

Next, the lawyers often take up some sort of reflective practice. Stress may lead a lawyer to meditate or practice yoga, as thousands of lawyers have done. Reflection quiets the busy lawyer mind enough to begin to reflect on important questions about life. Music, art or other forms of self-expression may also provide opportunities for reflection.

Mindfulness meditation is a hot trend for lawyers. At least a dozen law schools now teach some form of contemplative practice. Law firms, bar associations, and independent groups offer opportunities for group meditation in many communities around the world.

But, integrative lawyers can't stop with this.

Purpose and values

Taking time to quiet the chaos of the lawyer-mind, often leads a lawyer to start identifying her own purpose and values, and asking the questions that lead to living aligned with those values. I recall that my own reflections led to identifying myself as a peacemaker... and then asking how in the world could I design a law practice based on that? The question led me to explore not only my own purpose and values, but those of my clients, as well. I added questions to my intake forms, such as: What are your most cherished values? Knowing this, I was much better able to represent what was important to my client, not just what he could get in a case, but what would reflect what he or she actually wanted.

Thinking systemically

Something happens next that may not be quite linear, but I've seen it happen many times, so I recognize the evolutionary leap. We begin to think systemically, seeing interconnectedness and adopting new ways of thinking about how we impact each other. Many of us are on a quest to find the pivot points where small change can lead to big shifts. Integrative lawyers realize that every conflict has many stakeholders and began to look beyond the presenting issues, to deeper cause and effect. We recognize that society is becoming more complex, and that it is necessary to embrace the complexity while seeking to make the law understandable and workable.

Harbingers of a new cultural consciousness and leaders in social evolution

Integrative lawyers are leaders in an integral worldview which honors the wisdom and
best parts of all previous worldviews, while embracing emergent new ideas. Integrative lawyers bring this consciousness into the law and are partners with our colleagues in other disciplines. We are open to exploring and drawing upon many disciplines and wisdom traditions, such as, philosophy, science, metaphysics, psychology and spirituality.

Integrative lawyers default to collaborative approaches to problems, but are not afraid to take stands. We see that collaboration and cooperation are more workable than divisiveness and polarization. We understand that full self-expression can lead to conflict, and that, when approached consciously, can be prevented or resolved in ways that are productive and preserve the relationships between all stakeholders. We don't have to agree on every issue to be kind to each other and grant dignity to life.

**Becoming the changemakers**

At this stage in the process, it is a natural progression to adopt or invent new models of practicing. I am always inspired and amazed at the creativity of lawyers. Often similar approaches will emerge simultaneously, without contact between the inventors. For example, the trend toward using images in legal documents has originated on three continents which I can identify. Using multi-sensory legal tools for educating clients arose synchronously, too.

**Our numbers**

We really don't know how many integrative lawyers there are. The term is new enough and the group is emergent enough that many of the most "integrative" are not even aware of the label. In my travels, I meet them all the time. They often find me on the internet and write to me. Sometimes they show up at conferences or trainings. I can tell you this: there are more than you think and we are not alone. I know that because I meet more of them than I ever imagined, and I started out pretty optimistic. And we're a pretty diverse crowd, covering the globe, all practice areas, and a lot of personality types.

In August 2013, the *ABA Journal* published an article with the headline: "Is the integrative law movement the next 'huge wave' for the legal profession?"

**Challenges**

There is a lot more to the transformation of the legal profession than just adopting another model. While I previously thought the key was peacemaking, I have met litigators who have clearly transformed their lives and practices in ways that felt integrative and evolutionary.

Being integrative is more of an issue of deportment and the unseen. A lot of what it takes to be an integrative lawyer isn't what you learn in a classroom; it isn't like the bar
exam where analytical knowledge is measured. It isn’t a certification or a list of books someone has read. How do you measure listening? How do you measure creativity or emotional maturity? What tools tell us about consciousness? We can recognize when someone is connecting with us, but we don’t necessarily have measures to gauge that. I have encountered many lawyers who had not made the paradigm shift, who took the integrative procedures into four-way meetings without also bringing the mindset.

The process of evolution feels slow to those who envision a better world, but with consistency and determination, momentum can be reached. I compare it to riding a bicycle up a steep hill. We undertake that hill in our personal lives and in our practices. We may put in a lot of effort in the beginning, but eventually we reach a point where something shifts and we can move faster. Soon, we’re gliding down the hill, not sure why it took so much energy to get there.

**About the Author**

**J. Kim Wright** is a leader and storyteller for the integrative law movement. Recognized in 2009 as an ABA Legal Rebel, she has written *Lawyers as Peacemakers, Practicing Holistic, Problem-Solving Law*, a 2010 ABA best-seller, and *Lawyers as Changemakers, The Emerging International Integrative Law Movement* (ABA, 2016). Follow her on Twitter [@cuttingedgelaw](http://twitter.com/cuttingedgelaw).
Bringing Creativity to Legal Operations

With Stephanie Corey, by Nicholas Gaffney

Stephanie Corey is the chief of staff and legal operations senior director at Flex, a global electronics manufacturing company. Stephanie has spent the better part of her career providing value-added services to legal departments, including building and deploying critical infrastructure to enable them to meet their business priorities. After starting her career with Merrill Lynch, Stephanie worked for other financial services firms before moving to Hewlett Packard, where she worked for 11 years as the financial/legal operations manager for the legal department.

Her most recent role at HP was chief of staff to the general counsel, responsible for managing the daily operations of the legal department. Since then, Stephanie has started two small companies, including her legal consulting business and Miss Stephanie's Potions/Creole Labs, which make children's products. Stephanie is also the co-founder of CLOC (Corporate Legal Operations Consortium), a leading trade organization for information about legal operations and connections to the best legal operations professionals in the business.

Nicholas Gaffney (NG): What projects or ideas have you been focusing on recently?

Stephanie Corey (SC): We have several things currently underway. Because we recently rebranded and repositioned Flex (formerly Flextronics), we are undergoing a legal department transformation to support the ever-changing needs of our new businesses. The result is a complete reexamination and potential overhaul of how we presently offer legal services, and how our offerings need to change to meet our new, nontraditional businesses. This is an all-hands-on-deck project. Operationally, we are in the second phase of our contracts management implementation, we're diving deeper into spend analytics and looking at some new tools to do this, and continuing implementation of the efficiency initiatives we identified for each practice group at the beginning of the fiscal year. In the next few months I'd also like to renovate our website, both client-facing and internal.

NG: What could lawyers look at in a new way that would benefit their clients and society?

SC: This will be no surprise coming from someone who heads up operations, but I would like lawyers to be more willing to embrace technology rather than considering it a necessary evil that their clients are forcing up on them, and to consider being more transparent with information. The flow should go both ways between client and firm.

NG: If you could change one thing about the practice of law, what would it be?
SC: I would make the whole process less reactive. Outside counsel does the work for you, then a month later they send the bill. Hopefully, you’ve had discussions over the course of that month as to what the work being done was, what the bill will look like, and if they’re really on top of things, they would have put their accrual into your eBilling system so you can properly account for it. This process makes operations managers and the finance team sit around with our fingers crossed hoping for no surprises. I’d like to partner with the law firms up front to get immediate visibility into what’s being done, what’s being spent and what’s going to be billed so there are no surprises at the end of the month. The technology to do this exists, and I’d love to see law firms proactively implementing it and offering it to their clients. It would give them a huge competitive advantage.

NG: What is the most exciting development you have seen recently in the practice of law?

SC: I think the coolest thing I’ve seen recently is the technology that gives visibility into real-time data, which make financial planning, matter management, and reporting for our in-house attorneys a breeze. I’ve also seen some remarkable artificial intelligence tools that analyze your data for you, no matter what form it’s in, so you don’t have to rely on any type of manual coding. It makes reporting simple and accurate. The tech just keeps getting better and better.

NG: What technologies, business models, and trends do you think will have the biggest impact on the practice of law over the next two years?

SC: At the risk of sounding repetitive, I think we’re going to be seeing more transparency with law firms and in-house clients and the growth of technologies that support this, more use of data analytics and metrics, and more collaboration between the players in the ecosystem, such as technology providers, service providers, law firms, law departments and law schools, working together to elevate the industry.

NG: What’s the best new law practice idea you have heard recently?

SC: Of course I’m approaching this topic from an operations standpoint, but in the last couple of years, I’ve been working with some of the CIOs or COOs of the law firms to come up with creative solutions for some of the common problems we face (e.g. eBilling, the complexity of UTBMS codes, reporting, and quarterly or annual business reviews). In my opinion, these people are key to the future of legal services delivery, and law firms who don’t have this role (or listen to the advice of the person in this role) are already way behind. The people I’ve partnered with in this position are creative and collaborative and willing to work with in-house teams to solve problems. In fact, at the CLOC Institute in San Francisco a few weeks ago, I spoke to two law firm CIOs who had two completely separate ideas for projects that we could work on together. This role, with a creative person in it, make the law firm more progressive and gives them a significant edge over others.
How to Become a Cannabis Attorney

By Neil Juneja

Cannabis is the new hot topic of conversation, moving from the smoky dorm to the board room. The green rush is on, and, and, as any gold rush of the past, there is good business in selling the picks and shovels to those seeking their fortunes. Coupled with the most difficult legal market for aspiring and new attorneys in the nation's history, marijuana law is also a hot topic in law schools and in CLEs.

Marijuana is now legal for consenting adults in four states and Washington DC. Medical marijuana is legal in 23 states at the time this article was published. The international community is following suit, with an increasing number of nations decriminalizing or outright legalizing cannabis. Colorado now brings in more tax dollars from marijuana than from liquor. The momentum is clear; no matter which party conquers the 2016 presidential election, cannabis is here to stay.

While this nascent industry is growing at a pace unparalleled since the dot-com era, many large law firms refuse to service the clientele because the federal government considers marijuana to be a Schedule 1 drug, as defined by the Controlled Substances Act of 1970.

State v. Federal

Marijuana is still illegal federally. Some states have forged ahead with full legalization for adult use. These states have relied upon, inter alia, the Cole Memo, issued on August 29, 2013 by the U.S. Department of Justice. The Cole Memo informed federal prosecutors that state-regulated marijuana ought to be their lowest enforcement priority...but it is only a memo and nothing more. It can be disclaimed or ignored at any time.

While each state’s road to legalization varies, most states will study the experiences of Colorado and Washington in drafting their own laws and regulations. The familiar pattern has taken shape and suggests that other states will first move towards decriminalization. Second, they will permit medical marijuana for qualified patients. Finally, the state will legalize "recreational" marijuana for adults 21 and over. The state agency that regulates alcohol is usually the best choice to regulate marijuana for consenting adults, because the infrastructure already exists.

Practice Areas

Marijuana law, like entertainment law, is an amalgamation of other practice areas, including business law, administrative law, intellectual property, criminal law,
employment law and tax law. I would advise that any attorney targeting the cannabis industry should start with a firm foundation in business law. If the governing documents and contracts are subpar, you will very quickly sully the goodwill you earned with your current and future client base. Difficult tax and criminal liability issues arise when dealing with a federally illegal Schedule 1 drug having no [federally] recognized medical value. As the industry transitions from a subversive underground culture to a large and profitable legitimate industry, many unlikely business partnerships form. Before legalization, profits for the growers were substantial, owing mostly to the risk of criminal liability. In the emerging and highly competitive environment, profit margins are thin, and many businesses end up in litigation as the partners fight over shrinking margins.

Personal Knowledge

You should become adept in the subject matter. I am not advocating the consumption of large amounts of cannabis, or even any at all. However, you should know everything there is to know regarding marijuana. If you were to represent a liquor distiller, getting as drunk as the day after law school finals doesn't (necessarily) help the matter, but you should know how liquor is distilled, bottled, and sold, and the common business practices associated with the liquor business. With marijuana, you should understand the plant, the history, the extraction processes, active cannabinoids, terpene profiles, commonly used terms, and everything that goes into the product/medicine from seed to sale. Expect numerous tours of growing and processing facilities. Some of this knowledge will be technical and scientific, while some of it will more closely resemble folk magic. In either case, your clients and this billion-dollar industry take it seriously, and so should you.

First Impression

In every state on the path to legalization, marijuana is governed by brand-new regulation, modeled after systems that aren't quite analogous. This creates an issue that is unique to this area of law. The laws and regulations will change quickly and be applied inconsistently as the governing bodies learn and adapt to the subject matter. As a result, understanding of the law is not enough to best serve your clients. Working with the regulatory body to interpret and enforce the provisions is equally as important as understanding the legal texts. Marijuana law should not be an area to only dip your toe in. Plan to immerse yourself.

To excel in this industry, a cannabis attorney should become politically active. Your city government, state government, city attorneys, and police authorities are actively forming their cannabis policy. With the right approach, they may be quite receptive and work with you to get the laws and enforcement right. Help them understand your clients' issues and get to know the best lobbyists. Your clients will need them.

Partnerships
Many clients in the marijuana industry have no experience running a proper legal business. They will be lost and seeking your help in all aspects of starting and growing a business. Legal expertise is what we, as attorneys, provide. Not going further will be a disservice to your clients and leave them vulnerable to an industry that is far more competitive than any they have thus far encountered. Develop your personal relationships and open your contacts to your clients. They will need a location (real estate agent), accountant, security system, bank (if available in your state), master grower, extraction supplier, insurance agent, marketing company, packaging company, etc. Each and every one of these positions will need to cater directly to the marijuana industry to understand the nuances and quickly changing landscape. Be able to offer them contacts and let them know about any upcoming industry events so they can do their own networking.

**Ethics**

Does your state bar support a marijuana practice that is advises clients how to break federal law? Check the ethics opinions of your bar association or, if none exists, request an ethics opinion. If you are disbarred, you may be left with little choice but to grow fields of weed for a living. Determining if this is a better career path for you, I will let you discuss with your mom.

**Choose Your Clients**

It is very important that you choose your clients with care. Do not be afraid to send them to your competitors. Many of the most experienced people in marijuana are long-time criminals. All are criminals under federal law. Most often, veteran marijuana kingpins are rather docile. However, some of the people knocking on your door may be more dangerous and prone to shady dealing. Even organized crime is trying to get into the action. You will be working closely with the marijuana regulatory bodies and it is best to maintain your credibility for yourself and your clients.

**Off You Go**

Marijuana law is a fantastic but mine-filled practice area. If you are looking for something different, where you can help forge the laws, culture, and trajectory of an entire industry, there is nothing like it. Nothing is boilerplate and everything requires creative thinking. There is no place I would rather be.

**About the Author**

**Neil Juneja** is a registered patent attorney and is the founder of Gleam Law, a cannabis-focused law firm with offices in Seattle and Oregon. He can be reached at [Neil@GleamLaw.com](mailto:Neil@GleamLaw.com).
Cyber Insurance: Panacea or Pandora's Box?

By Steve Embry

In late 2013, the infamous Target data breach was announced, and the world of cyber security changed forever. Faced first with the embarrassment of having to admit hackers had gotten not only credit card data but also encrypted PIN numbers from debit card customers, Target then faced regulatory actions and a substantial loss of business. Target was ultimately hit with multiple lawsuits from consumers and financial institutions seeking billions of dollars in damages.

Lost in all this was the news that Target might have cyber insurance for some of its losses, but even this was, at least in the beginning, far from certain. (Ultimately Target did recoup some of its losses through it insurance policies). So it will go in the brave new world of cyber.

Data breaches, accompanying damages and losses and the inevitable litigation have been all over the news lately. Target was joined by such well-known merchants as Niemen Marcus and Home Depot in suffering highly publicized data breaches and have been sued in the aftermath. What hasn't got as much attention, however, is the insurance implications of these breaches and losses, and whether cyber insurance will end up being the savior or part of the problem. Whichever it will be, over the coming years its safe to say that hard-fought litigation will ensue, not only with respect to the data breaches themselves, but whether and to what extent insurance covers the losses.

A little background. The most common way of transferring risk in America is through insurance: if a risk is insurable and insurance companies are willing to accept the risk, then risk is transferable. Most businesses at the very least maintain commercial general liability and directors and officers insurance. And while arguably these policies may apply to data breach losses, many carriers are now specifically excluding these losses from the traditional policies. Instead, more and more, carriers are offering specific cyber insurance policies designed to protect businesses from at least some data breach losses.

Because no standard form exists for these policies (they actually differ substantially from one another), because some of the policy language remains negotiable, and because the law and policy language interpretation may differ from state to state, what these polices actually cover will have to be defined through extended litigation. And as we all know, technology is constantly changing, giving rise to more and more different cyber risks. Add to this the fact that many insured think they have very broad coverage, while many insurers believe the coverage being offered is more narrowly defined, you get an explosive mix that will fuel lawsuits and claims for the foreseeable future.

Cyber and privacy insurance has been available on the market for the last decade,
allowing businesses to ostensibly transfer the risk of liability and losses for a data breach in which the organization's or customers' information is lost or stolen. Marsh Inc., a global insurance broker, has estimated that the number of organizations that purchased cyber insurance in the United States increased by 33% from 2011 to 2012, and increased nearly 32% in the first half of 2015, making cyber insurance the fastest-growing area of commercial insurance in the world. (See, for example, "Cyber insurance in demand after recent data breaches: banks, hotels, educational institutions buying cyber insurance," July 28, 2013, CBC News).

In fact, the overall written gross cyber insurance premium is estimated to top $2.5 billion in 2015. The policies vary, with cyber insurance offered as a stand-alone policy, or as an add-on or included in more generally policies.

Two recent surveys, the Advisen Cyber Liability Insurance Marker Trends Survey and the Advisen Information Security and Cyber Liability Risk Management White Paper, demonstrate the shift toward cyber insurance and highlight the legal issues that may be just over the horizon. These surveys confirm:

- "The demand for cyber insurance is increasing and the insurance market is responding by adding new capacity and coverage."
- "The cyber insurance market has grown to over $2 billion, with industry prognosticators expecting it to double by 2020."
- 61% of businesses surveyed now have cyber coverage.
- "[T]he cyber insurance market is disjointed and muddled by...inconsistent policy forms."
- "While the demand for cyber insurance is arguably skyrocketing, the industry's attempt to understand a consumer's risk profile...is currently causing some confusion."
- Social media, cloud services, IoT and mobile devices are ever emerging risks. There are huge concerns about the security implications and exposure from these sources.
- The claims, risks, and coverages are evolving constantly.

So more and more cyber polices are being written, they contain different policy language and there is no form coverage. What does this mean?

For those not familiar with insurance coverage law and litigation, you need to understand that this law developed slowly over the years as different policy terms were created, reworded and dropped or added in light of the risks being presented. Gradually, the law evolved so that it was clear that certain language by and large meant the same thing. This gradual development was acceptable, since exposures and risks also evolved relatively slowly as well. This process provided some level of certainty for the carriers—who were pricing the policies and evaluating the risk—and the insured, who knew what they were buying. This is why most standard policies today by and large say the same thing.
But when a new area of coverage develops for new and changing risks and where no standard policy language exists, to pardon the expression, all hell is likely to break loose. No body of law defines what certain terms mean. And different albeit similar terms could give rise to different and multiple meanings depending on the jurisdiction. We have found that policy language varies widely in definitions, and even what constitutes an insurable event and occurrence.

Since what the language means is now open, and the typical way of resolving disputed insurance policy language is through litigation, lots of coverage disputes are likely in the near future. "As time passes, we may see more litigation in this area," said Nigel Pearson, global head of fidelity at Allianz Global and corporate Security, in a new report, A Guide to Cyber Risk: Managing The Impact of Increasing Interconnectivity. "There will be uncertainty about how courts will interpret some of the concepts. This is not unusual with new products and will result in a body of knowledge for underwriters." Industry representatives already privately predict they will be grappling with these problems the rest of their careers.

And of course, with coverage disputes come the inevitable bad faith claims, which up the ante and exposure. Given the unsettled nature of the law, even more opportunity may exist for these claims to be made.

While it's impossible to predict all the issues that will arise as these losses and claims proliferate, it is easy to see that they will be multiple and hard-fought, given the risk and exposure. And it doesn't take long to come up with just a few issues that themselves could easily fuel a decade's worth of litigation:

- Will business interruption losses be covered? One of the biggest financial hits taken by a breached party is for business interruption or lost profits—just ask Target. Generally speaking, the insurance industry is not eager to extend coverage for these losses due to the risk of large losses. And insureds often fail to address this up front assuming that these losses are covered. So when a loss occurs and this becomes an issue, look out.
- Insurance coverage ramifications often stem from the use of cloud computing or other vendors for hosting and processing data. Some cyber-risk insurance policies available today reflect the fact that the insured delegates this function to third parties. Some don't. But again many insureds may assume they are covered.
- Some cyber insurance policies condition coverage on the policy-holder having employed "reasonable" data security measures. Insureds will claim these clauses are so vague and subjective that they can't be enforced. And, given the speed of technological innovation and ever changing nature of cyber risks, what's reasonable just months ago may look less so in hindsight. Suffice it to say, as a general proposition, carriers will focus more and more on insurance application responses and use them against policyholders to contest insurance claims. Such arguments are notorious for leading to protracted coverage fights.
- Will the coverage include expenses of responding to informal inquiries and formal
proceedings that ensue from state attorneys general, the Federal Trade Commission (FTC) and others when a breach occurs? The recent case of FTC v. Wyndham, T.C. v. Wyndham Worldwide Corp., No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) in which the FTC data breach/privacy regulatory and enforcement authority was upheld, highlights another element of data breach damage since the regulatory actions stemming from a breach can generate millions in costs. The FTC has been pursuing these enforcement actions for years, and will be even more aggressive now. Will the policies cover cyber-related regulatory actions and the FTC enforcement of alleged cyber security failures that lead to breaches of consumers' personal information? Will coverage be limited to defense costs, as opposed to also covering fines and penalties? Traditionally, fines and penalties often were not covered under CGL policies, but who knows under the new cyber policies.

- In addition to fines and penalties, the FTC often seeks injunctive remedies, such as requiring companies to submit to security audits for a period of up to 20 years. Such remedies obviously cause companies to incur significant costs, yet the "Loss" definition of many cyber policies is also written to try to exclude such relief.

- Some cyber-policies offer regulatory coverage only through an add-on endorsement that must be purchased on top of a standard-form policy that contains a regulatory exclusion. When coverage is added by endorsement, there can be arguable ambiguities because the endorsement, which is not a standard form, may not line up perfectly with the underlying policy.

- Will the policies cover breaches arising from mobile devices that may or may not be connected to the company's computer network? More and more employees can access systems through tablets, smartphones, and PCs; some employees may unknowingly create security risks, even when the device is not logged onto the company servers. Will losses from this kind of breach be covered?

- How will courts treat notice requirements under cyber policies when there is a breach? Unlike other types of events, every second counts when dealing with a breach and mitigation issues may arise where notice is not promptly given.

- Some policies contain exclusions that specifically apply to certain alleged violations of statutes or regulations. This could be troubling in the data breach context, particularly since what is a violation in some states is not in others yet the applicability of various state laws can be quite broad depending on where a company does business. And what about the costs of notice under the varying state statutes? How will this be treated?

- How will the definition of a "claim" be treated? Cyber-insurance liability coverage usually is triggered by a "claim" made against the policyholder. Even when the "claim" definition encompasses a regulatory "proceeding," it may be limited to "formal" proceedings and actions "commenced by the filing of a notice of charges, formal investigative order or similar document."

- What about sublimits? Cyber policies often limit regulatory coverage by imposing "sublimits" that drastically reduce the amount of coverage for regulatory and other claims; in some policies, the regulatory sublimits may be a quarter, or even a tenth, of the aggregate limits. But ambiguities and inconsistencies can arise
when the sublimit is compared to the overall coverage.

- What do the policies say about coverage for consumer or business credit card information breach? These can be large exposures when there is a significant data breach.
- What about costs associated with ransomware? Insured will claim they have little choice here: pay or be shut down, and that this is just another cost of doing business. Will these costs be covered? Even if not, will the associated investigation costs and business interruption losses if the ransom is not paid be covered.

These are just a few of the more obvious issues. Given the plethora of policies and policy terms in the marketplace that even still are evolving, countless other issues will no doubt arise. And the evolving nature of devices and applications together with constantly changing cyber threats will also lead to new and unexpected insurance demands and coverage claims. So what these polies mean and what they cover could be a litigation issue that's not going to be resolved for quite a long time. Fasten your seatbelts, folks, we could be in for a wild ride.

**About the Author**

**Steve Embry** is a partner at Frost Brown Todd LLC in Louisville. He focuses his practice on class action, privacy, and mass tort litigation.
Dr. Roland Vogl is executive director of the Stanford Program in Law, Science and Technology (LST) and a lecturer at Stanford Law School. He focuses his efforts on legal informatics work carried out in the Stanford Center for Legal Informatics (CodeX), which he co-founded and leads as executive director.

Nicholas Gaffney (NG): What projects or ideas have you been focusing on recently?

Dr. Roland Vogl (RV): CodeX: The Stanford Center of Legal Informatics focuses on discovering and developing technology that can streamline and mechanize legal processes. Our main goal is to build a better legal system for all stakeholders. With regard to legal professionals, our goals are to help them deliver faster, better, cheaper and accessible legal services to clients. We believe these tools can help all clients, whether they are leaders of the global business community or low income individuals who cannot afford even basic legal services.

We have been building a robust, international community of people who are passionate about bringing information technology to the legal system, including "lawntrepreneurs," legal tech executives, scholars and students. We're bringing the community together at our annual CodeX FutureLaw conference and other live conferences, weekly meetings (live and online), and we have just launched our first "Open Innovation Challenge-Docket Analytics" in partnership with Thomson Reuters.

NG: What could lawyers look at in a new way that would benefit their clients and society?

RV: 1. The billable hour needs to be retired. Lawyers need a better way to show that we're providing value to the clients. This is, of course, not easy to do, but many lawyers are already adopting new, creative ways to better serve clients in their respective practice areas.

2. We need to proactively look for processes and technologies that help lawyers better serve clients with legitimate legal needs/claims. Today, 80% of Americans cannot find or afford legal services for non-criminal crises, and most citizens (including lawyers) don’t realize that there is no right to counsel in a civil case, as James Sandman, the president of Legal Services Corp., said recently.
This also applies to contingency-fee-based legal representation. For example, individuals injured by a product, or malpractice or corporate malfeasance—who cannot get legal representation because their injuries were not completely debilitating and the lawyers wouldn't risk investing time and costs for experts. Another example: the millions of mutual fund owners who regularly receive class action notices, where submitting a claim to join the class action is just too challenging—because they must prove every single trade with dates they occurred. These are very often, at their core, information problems, which can be solved by legal technologists. But they also need the various stakeholders (e.g., financial institutions) to provide the data in easy, accessible formats.

NG: What one thing about the practice of law would you change if you could?

RV: The billable hour—it creates an incentive to drag out matters; rather than to quickly and efficiently resolve issues. It's not surprising that many firms are going "boutique" and offering results-triggered alternate fee agreements and other options. Taking a "concierge" approach, where the goal is to create a long-term relationship with the client, builds trust—and steady payments.

NG: What is the most exciting development you have seen recently in the practice of law?

RV: A wave of innovation has built up over the last couple of years. It's not only affecting the practice of law, but the entire legal system. For example, law firms serving startups are experimenting with making many documents accessible for free, and providing legal information online. Firms are joining legal marketplaces to connect with clients and seem more sensitized to becoming more efficient to meet their clients' needs. The government is making legal information more accessible, providing legal data structured to be more accessible by computers—which will enable a new generation of legal applications. That can only help the user citizens.

Large information provider companies are teaming up with research centers, such as CodeX, to spur innovation in our field. Thomson Reuters, for example, has teamed up with CodeX to engage with innovators from around the world through an open innovation challenge. As part of that, they are opening vast amount of court docket data for participants. We believe that this will lead to many new and exciting applications in the docket analysis space. (See "Open Innovation Challenge-Analytics".)

NG: What technologies, business models, and trends do you think will have the biggest impact on the practice of law over the next two years?

RV: There is much talk about Big Data Law, and bringing data scientists' tools to the legal system. Law firms and corporate legal departments can leverage these
tools to better evaluate litigation risks or their contract exposure, etc. An early player in this field is Lex Machina, which focuses on intellectual property litigation. But a number of other interesting companies are using data science and machine-learning in different legal contexts, from contract analysis to patent law, such as LitIQ, Beagle, Kira, and PatentVector.

These types of technologies will have a big impact on legal practice—certainly for Big Law. Then, new research tools will become more and more popular over the next couple of years, like Casetext, Ravel or DocketAlarm. Finally, new online workflows and intake-forms, which are less high-tech, but nevertheless very useful, will also have an impact on lawyers' efficiency in the near future.

In the long run, "computational law" technologies, which automate and mechanize legal processes and compliance, will have a significant impact on legal practice. Some of these technologies will be quite disruptive to traditional legal practice. But lawyers who know how to leverage these techniques to capture their knowledge and make it accessible to more clients at lower cost, will benefit from the advances of computational law.

On the business model side, I think that the alternative business structure (ABS), which has been spearheaded by Australian and British regulators of the legal profession, has the potential to accelerate change in the profession. The non-lawyer ownership of law firms, which ABS structures enable, could really become a driver for R&D investment of law firms in the UK and Australia. This is certainly something to keep an eye on.

**NG: What's the best new law practice idea you have heard recently?**

**RV:** Not so recent, but quite persuasive to me, is the "SeyfarthLean" Six Sigma approach at Seyfarth Shaw. The basic idea is to adopt the core principles of Lean Six Sigma process improvement with project management and tailored technology to provide legal services. Another player leveraging Lean Six Sigma principles for process management and quality control, is NovusLaw, which provides document review, management and analysis services for litigation and transactional matters.

In addition, it seems that both lawyers and clients can only benefit from the efficiency gains that virtual law practice can provide. See ABA TECHREPORT 2014: Virtual Law Practice.