

**2017 ITechLaw World Technology Law Conference
Chicago, United States | May 3 – 5, 2017**

*Written by Marina Aronchik, Senior Associate, Mayer Brown LLP
and Enrico Miotto, 2018 J.D. Candidate, Loyola University Chicago School of Law*

Conference Summary

Technology is evolving as quickly as ever. The acronyms and buzzwords are all familiar at this point—AI, the IoTs, robots, blockchain, autonomous cars, and so on. But is there something different, and even more disruptive, about these latest technological innovations? The present generation of technological innovation is already producing vast changes in our society, economy, businesses, and even in the legal profession itself. Even greater change could be yet to come.

Conference sessions touching on contracting discussed the opportunity for lawyers to draft with a view to how successful relationships in the relevant industry play out. Lawyers can evaluate seemingly perfect provisions based on litigation outcomes but also business incentives of both parties. They might learn that protections sought by their clients are unnecessary, will not reflect performance, or are moot because proving damages will be impossible. To learn about parties' business incentives, lawyers can start by understanding the industry trends and habits, they might turn to conversations with in-house counsel on the other side of the negotiating table and ask about in-house counsel's incentives and internal processes.

Technology will automate some legal services, and in the future, clients might expect to pay nothing for services like legal research. Lawyers must be on the lookout for new ways in which their abilities can add value to automated services.

Cyber security is a threat to all companies and can cause expensive losses, and lawyers can protect their clients by understanding the industry standards recommended by insurance companies offering cyber security policies and by learning from cyber forensics experts. The initial costs to develop defensible cyber security training for employees and documenting a response plan can pay dividends for the ever-looming threat of a cyber security breach.

Europe's GDPR changes how companies can obtain consent to use data, written disclaimers or implied consent through use are no longer sufficient. The change impacts the internet of things, which even includes the way a patient must consent to a physician's use of data generated by the medical device's monitoring of the patient. Lawyers will likely have to find workarounds by justifying processing and storage of data other than pursuant to consent.

The 2017 World Technology Law Conference provided an in-depth examination of these and other trends in technology and their implications. Following are summaries of each session.

Written by Marina Aronchik, Senior Associate, Mayer Brown LLP

Keynote: Cybersecurity and the Trump Administration

Dr. Michael Sulmeyer, Harvard Kennedy School Belfer Center for Science & International Affairs

Dr. Sulmeyer opened his keynote address by focusing on the Trump administration's delays in developing a cyber security plan. He believes the chief reason for the administration's failure to meet the self-imposed deadline for the development of such a plan is the administration's desire to reinvent the wheel with respect to cybersecurity. Dr. Sulmeyer argued that the Trump administration should move past the planning phase, which it can do by identifying discrete recommendations in the extensive work performed by prior administrations and the broader research community and converting existing recommendations into a concrete plan.

Dr. Sulmeyer reminded the audience that cybersecurity is not a new issue, though the extent of the issue (and the associated risk) is quickly growing with expansion of connectivity. In the absence of government regulation, it is critical for the market and individual companies to take active steps to mitigate against cybersecurity risks, such as by implementing two-factor authentication, controlling the networks, and hiring specialized security firms to provide appropriate guidance on security measures. Dr. Sulmeyer hopes we achieve a state where implementing cybersecurity best practices is similar to a seatbelt in the car – you would not buy a car without one.

Dr. Sulmeyer also suggested that companies and academics have a window to proactively develop a healthy and profitable regime that would clarify who is responsible for implementing cybersecurity measures (e.g., companies or their customers), what appropriate cybersecurity measures should be, and how we as a society can adjudicate cybersecurity risks.

Written by Marina Aronchik, Senior Associate, Mayer Brown LLP

Cool Technology and Where it is Taking Us

Moderated by Gereon Abendroth, Osborne Clarke

Richard Corley, Goodmans

Pietro Fringuelli, CMS Cologne

N.S. Nappinai, Nappinai & Co. Advocates

This panel discussed new technology in the areas of energy, sports, and the Internet of Things (IoT). Focusing on clean tech, Richard Corley spoke of the inevitability of disruption. He provided an interesting perspective that through clean tech, the energy field is about to become part of technology, changing the way in which the society operates in the process. The efficiencies of clean tech in general and renewal energy in particular are creating new jobs and economic activities, including in countries that we may not expect to be leading the charge in this area, such as China and India.

Pietro Fringuelli introduced many in the audience to the concept of e-sport. Proving that a picture is worth a thousand words, he shared videos of e-sports tournaments, which are emotionally charged events that attract thousands (if not hundreds of thousands) of spectators, similar to what we expect with traditional sports. Unlike the traditional sports, however, the e-sport eco-system is largely unregulated.

In contrast to the exciting developments in clean tech and innovation of e-sports is the dark side of IoT or, more specifically, security issues associated with connected devices and the lack of meaningful regulation in this area. N.S. Nappinai discussed significant cybersecurity vulnerabilities that have been discovered and exploited over the past couple of years, including the attacks that brought down social media sites, like Twitter and Spotify, and known security vulnerabilities in household devices (e.g., nanny cameras) and connected dolls. She argued that it is critical to develop legislation and rules that would set out security standards for IoT devices (including disclosure of vulnerabilities in IoT devices) and provide an enforcement mechanism through penalties for violations of applicable standards.

Written by Marina Aronchik, Senior Associate, Mayer Brown LLP

Cars, Cars, and More Cars

*Moderated by Mark Hayes, Hayes eLaw
Jim Adler, Toyota Research Institute
Joerg Kahler, GSK Stockmann + Kollegen
Marjorie Loeb, Mayer Brown*

In this panel, Marjorie Loeb focused on three key legal issues for connected and autonomous vehicles:

1. the importance of understanding the risks associated with these vehicles,
2. the complexity of interconnected vehicles, and
3. the levels of collaboration that will need to happen and continue through the lifecycle of the vehicle to address those risks, in partnership with technology companies.

Ms. Loeb believes that it is important for vehicle manufacturers to recognize that it will likely be impossible to eliminate cyber risk in the context of connected and autonomous vehicles and, therefore, it is critical to manage that risk appropriately. She analogized the new general of vehicles to medical devices, arguing that like medical devices, these vehicles should be regulated to provide predictability and protection in this area to various actors involved with the vehicles.

Jim Adler provided insightful business views on ethical issues that arise in connection with autonomous vehicles. He posed the question, “to whom is the car loyal?” and pointed out the multitude of actors who may interact or otherwise be involved with an autonomous vehicle, such as the driver, passengers, bikers, and the insurance company, all of whom may have divergent interests in the behavior of the car. Echoing Ms. Loeb’s thoughts, Mr. Adler noted new communities that are developing around autonomous vehicles, who need to come together to create a framework for dealing with the risks in this area, including massive amounts of data generated by and gathered from cars, to which he referred as the “datafication” of the car.

Discussing relevant regulations, Joerg Kahler provided an interesting data point regarding a new law in Germany that makes automated driving permissible. He acknowledged, however, that this is the only example of Germany legislating in this area. Otherwise, Germany has adopted an unusual (for Germany) position of “wait and see” as it relates to autonomous cars.

Written by Enrico Miotto, 2018 J.D. Candidate, Loyola University Chicago School of Law

What Went Wrong - The IT Project Failure

Moderated by Peter Ruby, Goodmans LLP

Sally Hughes, International Association for Contract & Commercial Management

David McIlwaine, Pinsent Masons

Craig Elson, Charles River Associates International

Sally Hughes explained a value approach to contracting that is superior to contracting only in anticipation of litigation. Currently, negotiation centers around control, compliance and post-termination effects; it focuses on allocation of, and protection from, risk. Instead, negotiations should take a value approach using contract technology, clarifying scope and goals of the transaction, engaging stakeholders, and establishing governance rules and collaborative mechanisms for measuring and monitoring performance. In one example, a company's employment contract displayed in comic strip format created a transparent exchange with its illiterate employees. In part, the misalignment between the actual negotiation approach and the optimal one is due to the shift in the mercantile world. It was previously dominated by goods and now is dominated by services. Contracting parties should seek to negotiate content that reflects the shift in the mercantile world, in this way a contract becomes an economic instrument with which to begin and improve relationships rather than just a legal weapon.

David McIlwaine discussed IT disputes increasingly going the route of international arbitration, confirmed by a survey. An average large IT project runs 45% over budget, 7% over time, and delivers 56% less value than desired. Not only, 35% of all TMT disputes concern IT development, implementation and integration. 67% of all TMT disputes involve IT suppliers generally. In the next five years, data protection and system security breach disputes are anticipated to rise, surpassing IT development disputes.

Craig Elson described how to quantify damages in IT arbitration where they are commonly: unmaterialized benefits/returns expected when parties invested to deliver/acquire IT systems. At the outset, a damages calculation must identify any contractual remedies and limitations, such as those concerning liquidated damages, indirect and consequential damages, and ceilings to indemnification. Also important is any mitigation of damages, and any contributory negligence. The calculation must account for the nature of damages, from both vendor and customer perspectives. The vendor might experience damages such as cost overruns, expenses not contemplated and originating from the customer, and lost opportunities. The customer might experience damages such as delay costs, lost profits, unrealized savings, costs to replace failed IT, and incremental costs. Finally, a damages calculation often engages an IT expert and an economic expert and thus it must contemplate a direct causal link between the former's identified technical liabilities and the latter's identified damages.

Written by Marina Aronchik, Senior Associate, Mayer Brown LLP

Interactive Workshop: Changing Paradigm of Contracts/SMAC Platforms

Anand Bhushan, Shardul Amarchand Mangaldas & Co

Anand Bhushan provided a unique perspective on the disruption in the traditional market segmentation, emphasizing that over the next few years, companies will be looking for ways to identify savings through robotics and artificial intelligence. While that trend will likely lead to development of innovative technology, it is also leading to increased volatility of companies and difficulty in maintaining and growing traditional employment. Advances in technology are making it increasingly difficult to up-skill and retain (or reemploy) the current workforce.

The focus of the discussion then shifted to blockchain and artificial intelligence. Mr. Bhushan facilitated an engaging discussion of the effect of that technology on the legal profession and the impact of this technology on development and enforcement of appropriate service level agreements, among other aspects. In response to a question, Mr. Bhushan also weighed in on future development in technology, expressing the view that despite the high volume of technological advancements (such as virtual reality), these developments have been rather incremental, and that future developments will likely need time to prove themselves.

Written by Enrico Miotto, 2018 J.D. Candidate, Loyola University Chicago School of Law

Interactive Workshop: Technology "Contract-a-thon"

Kevin Woolf, Seyfarth Shaw

John Duggan, Seyfarth Shaw

The presenters discussed how companies use the project management approach of Lean Six Sigma to increase the efficiency of their transaction negotiations. Lean Six Sigma uses the three P's approach: process, platform, and people. "Process" refers to a company's standard protocol. In contract negotiations, it starts with intake and ends in storage. "Platform" refers to technology or software the process uses. "People" refers to participants of the process.

To improve "process," participants complete an interactive exercise in which they identify steps in a process and write each one on a sticky notes. Then, the notes are listed in sequential order and arrows are drawn to connect them. The details process map can then be made efficient by consolidating sub-processes, for example, identifying that early involvement of certain people can allow a company to eliminate later sub-processes. Also, bottlenecks or mundane sub-processes ripe for automation might come to light. Before mapping a process, lawyers often are not aware of hidden steps or sub-processes that colleagues implement as part of their processes. After the mapping, all participants gain a comprehensive understanding of the process and thus can collaborate to streamline it.

This process map could be done using a software such as TaskMap, a Microsoft Visio add-on. Processes created in TaskMap can link a user to company documents that could serve as guidelines at each sub-process. New participants can use processes in TaskMap to learn how their discreet role fits within the larger process. Lawyers can also use process maps to explain to clients how a firm estimates litigation costs, a litigation process map can show that difficult to predict events might force a more complicated litigation process. As an example of a company using this tool, Nike applied Lean Six Sigma to its IT contract management process. Initially, Nike's average turnaround time, from initial contract request to approval, was two weeks pre-Lean Six Sigma implementation was 2.6 days post-implementation.

Following this presentation, all participants received a hypothetical situation and worked in groups to map the process.

Written by Marina Aronchik, Senior Associate, Mayer Brown LLP

Data Fever: The Commercial Exploitation of Data

Moderated by Michael Isler, Walder Wyss Ltd

Rajesh Sreenivasan, Rajah & Tann

Nicolas Grunder, ABB

Dimitri Timmer, Microsoft

This panel discussed a variety of legal issues related to the commercial exploitation of data. The discussion started with Rajesh Sreenivasan sharing his views on the relation of rights to data to intellectual property rights and engaging the audience by asking us to weigh in through an interactive survey on the legal debate about ownership and rights to commercial exploitation of data. Mr. Sreenivasan then highlighted a recent case in Singapore involving Global Yellow Pages and the value in and rights to data. Interestingly, the judge considering that case concluded that there was no inherent value in data of Global Yellow Pages; rather, the value of the data came from analytics. Although it seems reasonable to conclude that there is no inherent value in otherwise-publicly available information, the Global Yellow Pages case raise the issue of whether, for example, a large pharmaceutical company can enforce its rights to data against third parties trying to use such data without permission, or whether its rights could be enforced only as it relates to the analysis of such data.

Dimitri Timmer and Nicolas Grunder discussed various scenarios of Microsoft and ABB using data and data analytics to improve their services or offer new services. For example, Microsoft could use data to predict when a machine may break down, providing added value to customers, as compared to reactive maintenance.

Written by Enrico Miotto, 2018 J.D. Candidate, Loyola University Chicago School of Law

Data Protection Differences: Big Data in China, Europe’s GDPR, Brexit, and Brazil Update

Moderated by Aravind Swaminathan, Orrick

Kristin Forde, Bull & Co

Nigel Parker, Allen & Overy LLP

Renato Blum, Opice Blum, Bruno, Abrusio e Vainzof Attorneys at Law

Grace Chen, Covington & Burling

The panel presented a comparative discussion of specific data protection issues in the US, Brazil, China and Europe. An expanded concept of personal data has been adopted in general by these countries: every datum that makes a person identifiable. In general, personal data requires an express, free and informed consent before collection, use, storage, or sharing.

As to Brazil, if at least one data processing step occurs on Brazilian soil and related services are for Brazilian users, then national legislation must be followed even by foreign entities. In general terms, Brazil imposes no restrictions on international data transfer, as long as rules are followed of the jurisdiction where data is stored. There are strict standards for security and confidentiality of personal data. Current law will be replaced by law modeled after Europe’s GDPR and the Canada’s PIPEDA. Unfortunately, differences in data protection and privacy regulations in different countries sometimes cause conflicting compliance requirements. For example, consent is treated differently in different countries. The US has the most flexible and lenient requirements for consent, there are several ways to get consent, and there is no requirement to opt in or out. In Europe, on the other hand, consent must be unbundled from other terms and conditions, it must go to specific individual consent, and it must be clearly distinguishable. Consent cannot be obtained with a “take it or leave it” approach. A supplier adhering to Europe’s GDPR can’t make consent a condition for providing a service. GDPR necessitates that a customer have the choice to opt out and nevertheless receive the service. In GDPR governed employment relationships, employees cannot give genuine consent because they are in an inferior bargaining position. In China though, consent from employees is automatically implied by the very existence of the employment relationship. And, the employer may not share the information concerning its employees with anyone. GDPR governed devices without screens, including a heart-rate monitoring wrist device or a sleep apnea device, create yet another consent issue. These devices collect information about the user but they do not have an interface from which the user can read text and therefore the user cannot deny consent. There is still uncertainty as to how new legislation will take these issues into account and how these issues play out.

Written by Enrico Miotto, 2018 J.D. Candidate, Loyola University Chicago School of Law

Practicing Law Ethically in 2030: How Legal Tech will change the Game

Niko Haerting, Haerting

Menno Weij, Solv

Jenna Karadbil, Law Office of Jenna F Karadbil

Diego Fernandez, Marval, O'Farrell & Mairal

Bill Brooks, Globality, Inc.

Jenna Karadbil discussed ethical issues impacting practice, especially competency and confidentiality. Judges in the US commonly order sanctions when lawyers fail to consider ethical obligations that accompany technology. Some US jurisdictions mandate lawyers stay abreast of benefits and risks of technology for providing services, for storing or for transmitting confidential information. California governs e-discovery skills that a lawyer must possess, and if a lawyer does not have certain e-discovery skills, then he or she must associate with somebody who does. California has repeatedly sanctioned attorneys for failure to properly supervise junior attorneys where technological carelessness impacted a case. Regarding confidentiality violations, 30 US states have rules requiring electronic communications or cloud storage to include reasonable protection. It is often an ethics violation, and not a reasonable protection, if an email includes only a comment to the effect of, "If this isn't for you don't read it." As to technology use in the legal practice, a recent sentencing algorithm failed because it could not consider ethics guidelines; it sentenced a 17 year-old who had sex with a 16 year-old more harshly than a 36 year-old because it reasoned there increased likelihood of recidivism in the 17 year-old.

Bill Brooks is part of Globality Inc., which uses technology to enable small and midsize providers, such as law firms, to participate in the global economy. Change comes more slowly in the legal profession than in the world outside, and legal ethics are playing catchup. The largest firms now have more lawyers thirty years ago, and they typically have offices in multiple jurisdictions. Lawyers from small and midsize firms want technology to find clients from other countries, help with client-lawyer collaboration, and help firms receive payment across borders. Artificial intelligence will enable a client with a particular legal problem to find and retain the right lawyer, and the desire for tighter security inhibits a lawyer's ability to harness technology to communicate and deliver legal services. More jurisdictions must accept a trade-off between how secure something can be and how useful it is.

Menno Weij discussed VraagHugo "Ask Hugo," a virtual lawyer that helps entrepreneurs without legal backgrounds to customize contracts. For example, VraagHugo asks a series of questions to an entrepreneur and then generates an NDA. It is inevitable that technology like VraagHugo and others will play an ever more prominent role in the legal market. This is not a negative forecast for lawyers however, they can embrace technology and identify new areas for value-add. In the short term, automated services might still need a lawyer's oversight if they don't remain abreast of recent litigation.

Diego Fernandez discussed artificial intelligence and that it will not disrupt the legal market but rather it will evolve the market. Lawyers will find new roles with the advent of new technology and thus technology will complement their roles. IBM's ROSS is software that researches law and the lawyer educates the software while she uses it. Thus, ROSS's legal research skills improve.

Written by Enrico Miotto, 2018 J.D. Candidate, Loyola University Chicago School of Law

The Global Vendor Perspective: What Legal Issues Keep Them Up at Night

Eugene Weitz, SAI Global

Eric Notkin, CGI

Nikki Latta, Deloitte

Derek Zolner, Oracle

Brendan Heneghan, IBM

Eugene Weitz moderated a discussion with in-house counsel whom negotiate customer contracts which center on the tensions between provider and customer. In-house counsel is constrained by senior management and contract teams which track contract modification and have approval powers. In-house must obtain swaths of approvals or modifying providers' standard terms, for example, approval from operations, privacy experts and senior executives. Providers use such a process for scalability, finalizing thousands of contracts a year for similar services guarantees profit. It also ensures audit compliance and predictability. The presenters warned that customization increases the risk that delivery does not conform which ultimately increases the customer cost. In terms of projects that ended negatively, most started with contracts driven by the counsel of customers. Contracts contemplating transformation of systems, such as automating a customer's business practice, challenge the description of delivery at the contract negotiation stage. These contracts should allow a provider to change delivery with agility, and it can do so by focusing on creative ways that a customer will benchmark in a cost-effective manner. The contract must reflect the real way in which a provider can deliver. In negotiating risk allocation, customers' counsel should tie risk to revenue and should negotiate a contract that manages a day-to-day relationship between provider and customer. Customers' counsel should understand customer value drivers and then incentivize the provider to deliver. Turning to cloud subscriptions, market pressures have commoditized cloud offerings resulting in reduced cloud deal cycles; cloud subscription contracts with lengthy deal cycles cut into contemplated subscription term. Further, cloud offerings that offshore data management have workarounds where customers have regulatory burdens. Offshoring also reduces cost without oft-perceived security deficiencies.

Written by Enrico Miotto, 2018 J.D. Candidate, Loyola University Chicago School of Law

Interactive Workshop: Cyber Crime, Data Breach and Litigation

Sloane Menkes, PwC

Joe Turek, Chubbs

All companies are targets of cyber security and 85% of cyber breaches take an average of 5 months to discover. Breach defense could include a data breach response team with a tailored cyber security strategy. In-house counsel could head cyber security because regulatory and contractual obligations usually accompany a breach, including notification to affected parties and the insurer. In terms of preparedness, a company should run tabletop exercises. In-house counsel participates, along with anyone with an emergency management role. They gather to discuss simulated scenarios and assess response procedures.

Underwriting a cyber insurance policy starts with assessing a company's risk mitigation – the quality of a recovery plan. This plan should be periodically tested and have first responders, support of a PR firm to communicate the breach externally, participation of counsel for regulatory compliance (to avoid fines, third party claims and litigations costs), a hot-line to cyber forensic experts for detection and investigation, implementation of regular safety controls and safeguards (PGP encryption is the gold standard for protecting data communication), and training personnel on phishing scams. A comprehensive preparatory phase is costly, but an underwriter should scale requirements to company size. For example, mid-size businesses in retail or education do not implement a full preparedness program. However, an underwriter sees a red flag if the company has the attitude, "we have insurance, that's why we don't encrypt." An insurance policy itself should help with the plan by providing things like software suites or specialized teams that oversee setting up safeguards for the insured. Companies should be aware that policies are often "claims-made & reported," where claims must be filed and reported during the policy period.

Written by Marina Aronchik, Senior Associate, Mayer Brown LLP

Interactive Workshop Startup Law Clinic

Charles Mudd, Mudd Law Offices

Steven de Schrijver, Astrea Law

Jimi Allen, Bureau Gravity

Steven Lee, Opternative

This panel provided a fascinating combination of lawyers' and entrepreneurs' perspectives on dealing with legal issues related to start-ups and structuring law firm engagements in a way that is mutually beneficially to lawyers and their entrepreneur clients. To kick off the discussion, the attorneys on the panel described their experience of working with start-ups and provided an overview of a wide range of issues that tend to come up for start-ups, including selection of the right business organization structure, negotiation of appropriate employment agreements, protection of intellectual property, and development of appropriate privacy and security policies.

The entrepreneurs on the panel described their respective start-ups and explained how they each dealt with law firms and legal issues as their respective business evolved. They asked lawyers in the audience to consider creative alternative fee arrangements for start-ups, such as deferring fees until a start-up raises a certain amount of capital, or introducing a tiered rate model where the rates increase as the start-up grows. Mr. Allen suggested that law firms may want to consider adoption a subscription model, where they would provide periodic advice on issues a start-up may wish to consider. This would help attorneys stay in touch with their clients and help mitigate both the challenge of "you don't know what you don't know" and the challenge of resolving issues under emergency circumstances. Asked about key criteria in start-ups' selection of counsel, Mr. Allen and Mr. Lee agreed that time and access (meaning, accessibility and responsiveness, both virtual and geographical) of their attorneys is key. Pressed further, they stated unequivocally that age is not a factor in the selection of their counsel!

Written by Marina Aronchik, Senior Associate, Mayer Brown LLP

Artificial Intelligence and Augmented Reality

Moderated by Elinor Cotait, Mundie Advogados

The Use of AI in Legal Practice, Dan Jansen, Nextlaw Labs

Augmented Legality, James Gatto, Sheppard Mullin

Heather Buchta, Quarles & Brady

This panel offered terrific insight into artificial intelligence and the less-often discussed topic of augmented reality, including the legal issues that come up in both of these areas. The first half of the panel focused on the development of disruptive technology in legal practice. Nextlaw Labs is developing a sophisticated artificial intelligence tool in cooperation with Dentons designed to create a more efficient way of processing routine low-complexity legal work (such as due diligence). Additionally, there are a variety of other tools that are either already on the market or that are in relatively late development stages, such as Brexit Contract Review Solution (which helps companies work through the implication of Brexit) and Beagle (a contract analysis tool). In response to a question from the audience, Mr. Jansen shared an interesting and somewhat counter-intuitive perspective that, even though these artificial intelligence tools seem posed to reduce the volume of work that young lawyers are handling, the younger generation (college students or law students) are the ones who are most excited by these innovative tools. While it is too early to predict how these tools (and which tools) will prove to be the biggest disruptors to the legal profession, we can be certain that the legal profession will be evolving rapidly over the next few years.

The discussion then shifted to the world of augmented reality and the corresponding “augmented legality”. Mr. James Gatto discussed legal issues that arise in connection with augmented reality, using Pokémon Go as an illustrative example. A seemingly-innocuous game raises a stunning number of legal issues, including allocation of liability for personal injury and property damage, and applicability of traditional property rights (such as trespass or nuisance) and intellectual property laws and concepts. Mr. Gatto then introduced the audience to the only known piece of legislation concerning augmented reality, which is an ordinance in Milwaukee County, together with litigation that it attracted.