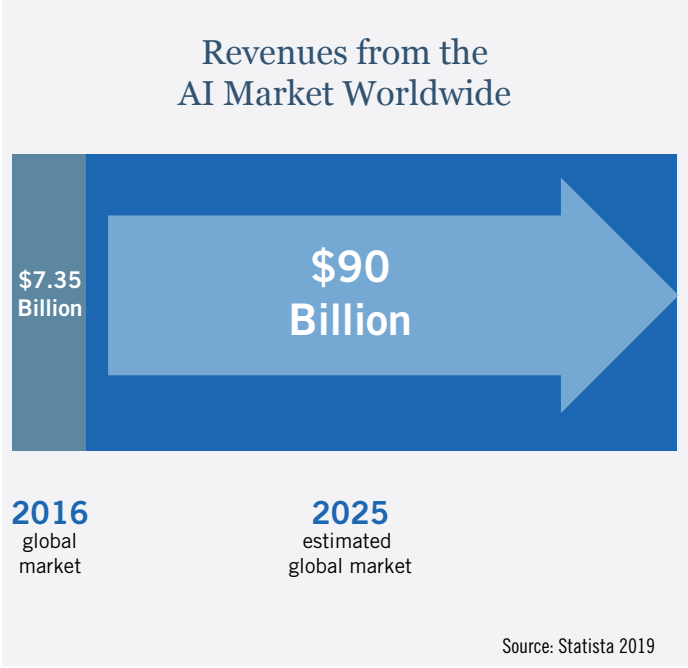
FOLEY

FOLEY & LARDNER LLP

AI is Here to Stay: Are You Prepared?

A 2019 Report Prepared by Foley & Lardner LLP
Explores Opportunities and Challenges

It seems as though a week doesn't go by without splashy news of an artificial intelligence (AI) company's technological breakthrough or massive funding haul. Even President Donald Trump drove headlines in February when he signed an executive order known as the American AI Initiative, which aims to encourage investment in AI and set governance standards, among other initiatives. The global market, already estimated to be valued at $7.35 billion, is expected to catapult to nearly $90 billion by 2025.



AI can help pathologists identify diseases, and physicians better assess brain health. It can help bankers automate back-office processes, create more lifelike chatbots and improve fair lending practices. It can process and collect data more efficiently, protect from cyberattacks and improve driver safety. And all of that is just the tip of the iceberg. As one security professional put it: "For large countries, growing and investing in AI is now a matter of national security and longevity. It's the next natural resource."

But developing AI safely, legally and efficiently is an uphill battle that — if navigated incorrectly — could result in a disappointing, if not outright dangerous, assortment of missed opportunities. That's according to Foley & Lardner LLP's conversations with numerous startup founders and high-profile executives working with AI. As **Thomas Fuchs**, founder of **PAIGE.AI**, put it, "In medicine, people die not because of AI, but because of the lack of it."

In lieu of any significant government guidance or regulations, the problems are complex and far-ranging — and in one way or another, all companies dealing with AI must ask themselves difficult questions. The following report provides key insights from our qualitative research. The hope is that those reading this — whether they're already involved with AI or are looking to be — will accrue the foundational knowledge needed to move forward and seize the promising opportunities before them.

The Dangers of Hype

It's almost standard practice for tech startups to claim they use AI. And while it's understandable why startups would tell lay audiences that they use this powerful new technology, most professionals we talked with questioned the accuracy of the startups' claims. In fact, most people who say they're using AI are actually using machine learning (ML), or if-then rules, decision trees and similar basic logic, the professionals said.

"These models can be very useful, they can be used to help fly a plane, for instance, or diagnose cancer," **Fuchs** said. "But they can't generalize anything else than what they're trained to. They can't reason like a human on new problems, like AI theoretically would. We're decades off from that."

And no matter what you mean when you use the term, the hype around AI can be potentially dangerous — because if one AI project fails (no matter how "AI" it may be), the rest of the field fails with it. At least, in the public eye.

INSIGHTS

Across disciplines, professionals strive for a certain amount of patience and due diligence. They encourage cross-function cooperation on AI and stress the importance of bringing in outside counsel — legal and otherwise — along the way.

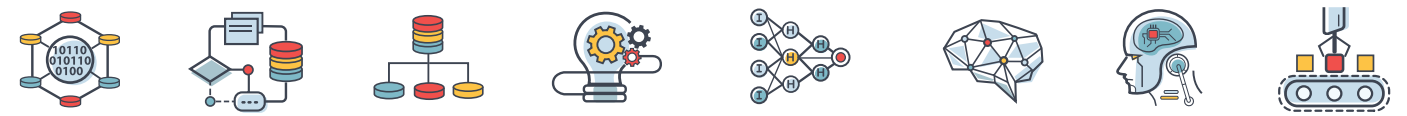
"The opportunities in AI and machine learning are endless and despite the desire to pursue numerous opportunities, it is the responsibility of the management team along with key stakeholders including our customers, regulators and counsel to take a step-by-step approach," said **Robert Hamilton**, co-founder of **Neural Analytics, Inc.**

Access to Quality Data

The promise of AI stems from the veritable flood of data coursing through our digital world. But as **David Chan**, senior patent counsel at **Western Digital Corporation**, said, "The amount of data needed for AI is substantially larger than what we're able to handle today. Think of automated vehicles, all the cars and all the technology necessary to support them. To make it work, every intersection will become a data hub. We're not ready for that."

Furthermore, the pace at which AI is being developed is likely dictated in part by the rate at which such inbound data can be handled, and new or modified algorithms are put in place. As Beni Surpin, a partner and technology transaction lawyer at Foley explained, "We can't expect just yet, for example, autonomous vehicles to know where precisely the prior night's snowfall has been shoveled, and how much lane space remains open. Think of it along the lines of a child's brain needing to learn to crawl, stand and walk, before that same child can process learning to ski, let alone ski off-piste in the trees."

On a smaller scale, there's also the matter of getting the right data and putting it in the right place. According to John D. Lanza, a partner and intellectual property (IP) lawyer at Foley, "AI hasn't changed the fundamental rule of 'garbage in, garbage out.' Data governance is important not only to how a company protects its data set, but also to how it stewards the data it has collected, usually from its customers. Make a mistake with data entrusted to you by your customers and you've just killed the goose that lays the golden egg."



Health care companies face their own challenges in utilizing AI. The Food and Drug Administration (FDA) is actively working with health care companies to ensure the safe and effective use of new AI technologies. Additionally, there are considerations with the Health Insurance Portability and Accountability Act (HIPPA), which need to be assessed by every company as they begin to harness the power of health care data, **Hamilton** said.

There's another problem with data that is used to train and validate AI algorithms. As Aaron K. Tantleff, a partner and cybersecurity and technology lawyer at Foley, noted, "As long as the training data is selected by humans, there will always be a selection bias. And, despite our best intentions, there is always a bias towards the data one selects." These biases impact the values used to train the algorithms. Ultimately, understanding this data bias helps to better design the algorithms by knowing the limitations of the data being used to train the algorithms. Failing to appreciate bias, or ignoring or dismissing it, can lead to dangerous consequences.

INSIGHTS

"Organizations that have large amounts of data may need to start with a comprehensive data-mapping exercise so they can understand what data they have and where it's located. Then they can start eliminating data that's no longer relevant or incorrect, and they can erect technical and organizational measures to ensure the remaining data's confidentiality, integrity and availability when and where they need it," said Steve Millendorf, a cybersecurity and privacy lawyer at Foley.

For startups, getting quality data often means partnering with external institutions. PAIGE.AI, for instance, partners with Memorial Sloan Kettering Cancer Center to attain images and develop its AI-powered pathology modules. But it's crucial, Millendorf said, "to make sure that data-sharing agreements clearly state who retains ownership of both the input and the resulting data, while also limiting the use of the data to just what is necessary for the services."

Jeff Gundersen, a partner and patent lawyer at Foley, said there are other considerations to keep in mind: "What can each party do with the data? Are there confidentiality obligations? Use restrictions? Also, are there geographic storage location considerations? If insights from the data lead to innovations, who owns those? If the data leads to incorrect conclusions, who is on the hook?"

An Uncertain Regulatory Landscape

AI technology is accelerating so fast that it's no surprise that regulatory bodies lag. There's the General Data Protection Regulation (GDPR) in Europe—although questions loom as to the fate of AI under the GDPR—as well as a slew of longstanding privacy, cybersecurity, unfair trade acts, due process and health and safety rules that cover technologies now considered to be AI. But no regulations or regulatory frameworks exist specifically for AI. Some say this is good — AI and its capabilities are still so vague that any regulation might stifle innovation. But our research shows that some broad parameters from the government would be helpful to those developing AI.

"We would like the option to innovate without restrictions imposed by regulators. But from a competitive standpoint, it would be good to have something like Obama's privacy principles, or what the FFIEC did with social media," said **Katie Licup**, vice president of enterprise privacy and fair banking at **Discover Financial Services, Inc.** "Something that says: 'Here's how we expect you to operate.' Then even unregulated entities would have to play by those norms."

INSIGHTS

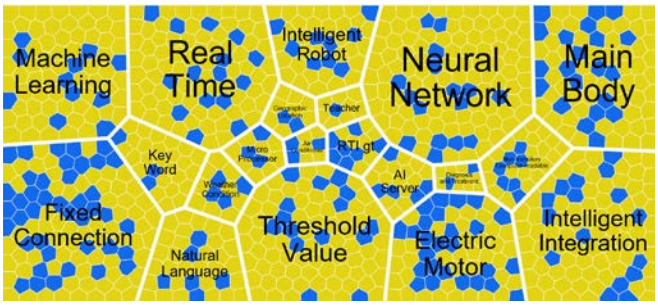
Dealing with regulatory uncertainty for AI varies across organizations and industries. For instance, **David Berglund**, senior vice president and AI leader at **U.S. Bank**, said, "It's about having conversations — with internal legal and risk teams, with various working groups and organizations — to better understand the shifting dynamics and to make sure we're not improperly restricted from realizing the positive benefits AI can deliver. A lack of regulations shouldn't — and doesn't — give us free rein on what we do, but we should instead be driven by: What's the right thing to do from an ethical mindset?"

Shabbi S. Khan, an intellectual property partner at Foley, said it's important to communicate with regulators. "Companies who work with regulators are better served as their solutions not only are compliant with future regulations but also used to formulate the regulatory framework and standards that other companies' solutions are evaluated on for compliance." **Licup** agrees and said it's also important to look outside of the regulatory space for guidance — whether it's the newly revised NIST Cybersecurity Framework or a big tech company's code of conduct.

The actions of big companies can serve as guideposts, said one executive. "We don't have an in-house regulatory team, so we rely on [outside] legal experts and look to see how Google and Facebook are dealing with regulations."

When it comes to health care, the focus is on the actions of the FDA, which many observers say has done a great job of ushering through clearances for AI and ML devices. This is promising — but clearance doesn't mean adoption. Health care startups using AI face significant hurdles when it comes to clinical adoption. "The reality of medicine," **Robert Hamilton** of **Neural Analytics** said, "is that you need clinical evidence to get adoption of the device."

Regardless of industry, there is something of a consensus around the hope, as **Karl Reichenberger**, vice president and assistant general counsel at **Johnson Controls**, explained. Reichenberger, who serves as lead counsel for Johnson Controls' Digital Solutions and Global Retail Solutions businesses, said, "I hope regulators will work with the buildings industry to understand the benefits of AI and to collaboratively achieve regulatory solutions that do not paint all AI with the same brush. At Johnson Controls, we believe our AI-driven solutions create more sustainable, insightful, productive and safe buildings."



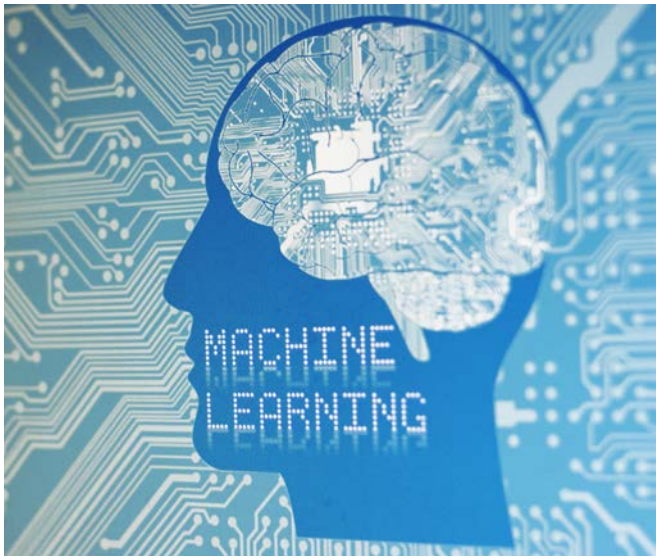
The Intellectual Property Conundrum

As with all AI-related concerns, IP is specific to each technology, use, industry and organization. With that said, we heard again and again about a primary challenge with patenting AI, especially in light of *Alice,* a recent court case on patent eligibility. **Michael Campos**, research scientist and director of IP at **NetraDyne Inc.**, explained, "The engineering process of designing AI is not so much about specifying a precise sequence of algorithmic steps. The engineer sets up an architecture for the problem and building blocks of the solution. The training algorithms then learn to select and blend different components into the ultimate algorithm. It can be a challenge to fit that into the typical form of a methods claim."

That is, for most AI, it may be difficult to patent AI's abstract processes in the United States. Meanwhile, **David Chan** of **Western Digital** said, Asian countries like China and South Korea have in contrast announced changes that would allow software to be patentable or give preferential treatment to certain AI patent applicants, and the European Patent Office issued patentability guidance on AI inventions in late 2018.

On the issue of IP, many thought leaders we spoke with discussed the debate over whether to patent their AI or keep it a trade secret. This is especially critical for some health care startups. "In medicine, the publication of clinical data is essential for clinical adoption of the final product," **Robert Hamilton** of **Neural Analytics** said. "However, this presents challenges for AI companies in the health care space as we must weigh the pros and cons of submitting an application or keeping the technology as a trade secret."

Although some companies hold off filing patent applications for AI innovations, Paul S. Hunter, partner and co-chair of the Electronics Practice at Foley, said, "The number of AI patent applications has dramatically risen in the past four or five years, reflecting the expectation of potential value of AI in the marketplace."



INSIGHTS

When it comes to patenting AI, many professionals suggest dividing the technology into two categories. "The abstract processes — the trainings/learnings of the technology — you may want to keep as a trade secret rather than spend money to try and patent it," **Chan** said. "The business applications of the technology, though, you can patent — you want to patent only the things in tangible applications."

He adds that the trade secret approach can fail you if another company can observe the inputs and outputs of your AI technology and figure out how you've arrived at the solution. **Reichenberger** agrees. "Before the Patent Office, I believe it is important to be realistic and fair with the scope of your claims," he said. "If claims are drafted to cover methods of thinking about conventional business methods, it will be difficult to discuss those claims with the patent examiner when attempting to demonstrate patentability. If, on the other hand, we claim an innovative technical solution for managing and controlling building devices in a new and energy efficient manner — a real solution to a real problem — we would hope to get past the subject matter eligibility question and on to the questions of novelty and non-obviousness."

Furthermore, companies should consider whether infringements of their patent claims are detectable. "Given that a lot of the AI innovations happen within the proverbial AI 'black box,' oftentimes it is hard to determine whether a competitor is infringing claims that are directed toward features within the black box. Such patents can be valuable, but patent owners should be informed about the challenges of detecting infringing behavior by competitors," Shabbi Khan of Foley & Lardner said.

Despite the importance of protecting AI IP, it's crucial that those in the space not isolate themselves. As **Michael Campos** of **NetraDyne** said, "We want IP rights, but we also know that if you try to do everything yourself and don't engage the outside, the field is moving so fast you'll be left behind."

Still, Jeff Gundersen of Foley & Lardner said that many sophisticated technology companies favor patent protection early on. "You can always license your patents to strategic partners in a particular field. But not protecting your own ideas is a fast way to marginalize your company."

For John Lanza of Foley & Lardner, it's a matter of simply knowing your business. "The cooperative nature of competition in the AI space requires one to have a clear view as to what constitutes the core value of the enterprise and what does not," he said. "That assessment needs to be revisited frequently to ensure the enterprise remains relevant."

More Data, More Privacy Concerns

With AI requiring massive amounts of rich data to operate, there are exponentially more privacy concerns to manage. "There is no 'one-size-fits all' rule that can be applied," Lanza said. "Everyone has their own view as to what data is sensitive and that view evolves daily."

To make matters more complex, the definition of personal data has changed. "In the past," **Katie Licup** of **Discover** said, "you could get by saying that an IP address wasn't personal. But now data can be attributed to such an extent that there's a privacy component even if the data isn't originally being used in a way that's personally identifiable."

"What's more," Millendorf said, "AI may make it even easier to re-identify someone from otherwise anonymous bits of data, raising new privacy concerns on the output of AI processes."

The massive amounts of data needed for AI will also require more sophisticated data governance models, as ownership rights in data are more challenging than what they may initially appear. Parties tend to think of data as a single item to be owned by one party and licensed under specific terms to the other party. However, in an AI ecosystem's data supply chain, data typically comes from a digital exhaust of a variety of sources, is consumed and transformed into derivative data items and is then provided to and used by different entities.

INSIGHTS

For **Licup** and others, managing privacy concerns is a matter of educating business partners. "We have to teach them that even an inference about a person for, say, a targeted marketing campaign could cause the consumer to ask: How did I get here? And then unwind to see where the data came from."

Safeguarding against privacy issues also means having an internal process that's diligent, cross-operational and efficient. **Reichenberger** said, "We have a number of privacy checkpoints in our product development process involving a variety of different functions. Legal, cybersecurity and privacy teams collaborate with engineering on each product going through our process." For instance, Reichenberger's company has a privacy impact assessment process, which touches multiple steps in the product development process and serves as the basis for a conversation and evaluation with the cross-functional team.

But while protecting data is incredibly important, **Hamilton** said privacy regulations — at least in health care — should reflect the reality that not all data is created equal. Thus, it's not only a policy issue but a cultural one as well.

The Double-Edged Sword of Cybersecurity

Bad actors have access to AI too, and the security effects could be disastrous. **Stu Sjouwerman**, founder and CEO of **KnowBe4**, which hosts the world's most popular integrated security awareness training, has been on the front lines for years.

"There's just so much data out there for hackers to use," **Sjouwerman** said. "It would be highly unlikely that bad actors are not using machine learning to some degree. They're extremely well-funded, and they only have to be right once. Five to 10 years down the line, we're going to see highly sophisticated AI battling it out on both sides."

"Cyberwarfare will ultimately be a battle of AI," Millendorf said.

According to Aaron Tantleff of Foley & Lardner, we are already seeing bad actors accumulate large data sets derived from breaches, as well as information that individuals make publicly available. Combining those data sets with the power of AI, bad actors can create attacks that are effective at levels previously unfathomed. And, these attacks are just at the early stages of implementing the power of AI. Since the bad actors are not bound by the same laws or ethics that the surface community is held to, their ability to advance this new threat outpaces our ability to defend against it or build effective tools to counter act these threats on a real time basis. Thus, it is critical that we look to AI to counter threats presented by bad actors, because if we fail to do so, we will lose the digital war.

Tantleff also points out the rising threat of adversarial data that bad actors are deploying. A bad actor needs only to make subtle, almost unnoticeable changes to the training data, which could undermine the way an AI algorithm works and cause unexpected outcomes, thus destroying the positive impact of AI. Undetected, this adversarial data could wreak havoc on the advancement of AI. Therefore, it is critical that companies ensure the security of their training data and their software.

Meanwhile, government movement on this issue has remained nearly stagnant, though legislation is currently on the table that would require security awareness training with frequent social engineering tests.

INSIGHTS

According to **Stu Sjouwerman** of **KnowBe4**, the only way to prevent these attacks is to train employees not to fall for them. That requires a shift in the cultural mindset toward security awareness.

"The human side of the equation has mostly been ignored because security awareness training had a bad rep," **Sjouwerman** said. "It fell into the cracks between HR and IT. HR didn't have the technical knowledge and IT didn't know how to train people."

The shift to a safer security culture needs to come from the top down. "If you can get sufficient cover from C-level executives," **Sjouwerman** said, "it can be done. Security needs to be rewarded; there need to be incentives for secure behaviors."

The Talent Gap

If AI is truly the next natural resource, then the need for talent and education around it will be crucial — both for large companies and startups alike, in every industry. It's a big, systemic problem that must be addressed by government, educational institutions and businesses alike. "If this isn't addressed by these three forces, we might see a slower rate of development and subsequent commercialization of AI in the marketplace, than what would otherwise be its true potential growth," Beni Surpin of Foley & Lardner said.

For now, one side effect of the shortage is that if you have a Ph.D. in machine learning, you'll have an offer from a big tech company before you even turn in your thesis. This leaves many startups, in the medical field, for instance, without the proper AI know-how.

INSIGHTS

Part of educating people on AI means encouraging, at least early on, a culture of openness and innovation. As one executive said, "It's like software — a lot of it should be in the public domain, where it can be made widely available."

Michael Campos of **NetraDyne** seconds that notion and is optimistic about the culture of openness around AI. For instance, he points out that when a prominent researcher and AI academic, Yann LeCun, was hired at Facebook, he kept his position at NYU. **Campos** explained that "it's important to keep one foot in academia. People want to get their name out and publish. You don't want to be stuck in the castle. The talent pool is too small."

For health care, the challenge is not only finding talent willing to reject huge salaries from big tech companies but educating physicians on the benefits of AI. Because they're not trained in data science, physicians tend not to understand machine learning processes — they mistrust the idea of putting data into a black box and receiving an output on the other side. They want to see the pathway, which means it's vital that health care AI companies take the time to show the levels of evidence and correctly design clinical trials.

And in the long run, **Thomas Fuchs** of **PAIGE.AI** said, "joint ventures make a lot of sense." He cites his tri-institutional approach — his lab, along with Cornell University and Sloan Kettering — as a model for inculcating a new generation of machine learning talent in the medical field.

"Joint venture agreements covering application of machine learning technologies and collaboration among multiple parties can quickly become complex," Christopher J. McKenna, a partner and co-chair of Foley's Electronics Practice, said. "Each party has an interest in the ownership of IP and data between the application, the machine learning technology models and components as well as the flow of data used as input to models, output from the models, and integrated into and used by the application."

Conclusion

The hype may not all be real, but AI is, and it's here to stay. Among leading executives and startup founders in the space, there's no doubt that, despite some uncertain and complicated terrain — around regulations, IP, privacy, security and more — AI will be the next technological frontier.

But let's get one thing straight: This isn't some science fiction movie, with a world suddenly run by robots. Many respondents stressed the importance of the human element when it comes to AI and how underestimating that would be as detrimental as underestimating the technology itself. AI, being created and modeled by humans, has the ominous potential to learn and reiterate our own human biases. On the other hand, we can't forget that AI technology is there to support human endeavors — to replace more menial tasks and allow us to take the reins on more complex ones. To expect the technology to do everything for us would be a grave mistake.

At the end of the day, AI, like all technology, is resolutely human. But that doesn't mean it can't improve society. If we seize the AI opportunity thoughtfully — with humanity, ethics, education, testing and due diligence across organizations and functionalities — perhaps we can, as **Campos** suggests, "make systems that are a little better than we are."

FOLEY

FOLEY & LARDNER LLP

KEY CONTACTS & CONTRIBUTORS

David Berglund
Senior Vice President and AI Leader
U.S. Bank

David Chan
Senior Patent Counsel
Western Digital Corporation

Robert Hamilton
Co-Founder
Neural Analytics, Inc.

Karl Reichenberger
Vice President and Assistant General Counsel
Johnson Controls

Michael Campos
Research Scientist and Director of IP
Netradyne Inc.

Thomas Fuchs
Founder
Paige.AI

Katie Licup
Vice President of Enterprise Privacy and Fair Banking
Discover Financial Services, Inc.

Stu Sjouwerman
Founder and CEO
Knowbe4

Jeffrey S. Gundersen
Partner

Mechanical & Electromechanical Technologies
Milwaukee
jgundersen@foley.com
414.297.5897
Profile

Shabbi S. Khan
Partner

Electronics
Boston
skhan@foley.com
617.502.3291
Profile

Christopher J. McKenna
Partner and Co-Chair

Electronics
Boston
cmckenna@foley.com
617.342.4057
Profile

Aaron K. Tantleff
Partner

Privacy, Security & Information Management
Chicago
atantleff@foley.com
312.832.4367
Profile

Paul S. Hunter
Partner and Co-Chair

Electronics
San Diego
phunter@foley.com
858.847.6733
Profile

John D. Lanza
Partner

Electronics
Boston
jlanza@foley.com
617.342.4084
Profile

Beni Surpin
Partner

Technology Transactions & Outsourcing
San Diego
bsurpin@foley.com
858.847.6736
Profile

Steven M. Millendorf
Senior Counsel

Privacy, Security & Information Management
San Diego
smillendorf@foley.com
858.847.6737
Profile

About Foley

Foley & Lardner LLP looks beyond the law to focus on the constantly evolving demands facing our clients and their industries. With over 1,100 lawyers in 24 offices across the United States, Mexico, Europe, and Asia, Foley approaches client service by first understanding our clients' priorities, objectives, and challenges. We work hard to understand our clients' issues and forge long-term relationships with them to help achieve successful outcomes and solve their legal issues through practical business advice and cutting-edge legal insight. Our clients view us as trusted business advisors because we understand that great legal service is only valuable if it is relevant, practical and beneficial to their businesses.

FOLEY

FOLEY & LARDNER LLP

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