St. John's Law

Magazine | Spring 2019

Special Report

WHO'S MINDING OUR DATA?

Privacy | Cybersecurity | Compliance

Special Report

WHO'S MINDING

OUR DATA?

ALUMNI WORKING AT THE FOREFRONT OF PRIVACY, CYBERSECURITY, AND COMPLIANCE

Alexa.

It's a name that echoes through millions of homes every day. Amazon's virtual assistant is on call 24/7/365 and, with just a voice command, will turn on the lights as we walk in the door, raise the thermostat, pay that bill we forgot about, and order a pizza for delivery so all we have to do is sit back, relax, and enjoy the latest *Game of Thrones* episode that Alexa recorded for us.

With all of those Alexa interactions comes a flood of information about the people engaging with her. That data joins streams of other data gathered and relayed as we go about our daily lives texting, online shopping, using our favorite apps, grabbing a ride share, and even opening our refrigerators, among other activities.

It's estimated that human beings generate as much as 2.5 quintillion bytes of data every day. By 2020, billions of connected devices worldwide will enable every person to create 1.7 megabytes of new data *every second*.

So it's no wonder that data is fast becoming the most valuable commodity in our economy. As the World Economic Forum has stated, "Personal data represents an emerging asset class, potentially every bit as valuable as other assets such as traded goods, gold or oil." Data's value comes from the wide range of insights it can reveal about people, places, and things. Those insights, in turn, are now more accessible and useable thanks to big data, artificial intelligence, machine learning, and other scientific advances.

As data, especially data in the form of personal records, has emerged as the world's most valuable currency, its vulnerabilities have become clear. Whether orchestrated by bad actors or caused by basic human error, data breaches are common and can shatter privacy, upend lives, and damage corporate reputations.

Responding to this threat landscape, U.S. state and federal regulators and lawmakers have created a patchwork of data protection protocols. And, recently, the European Union (EU) enacted its sweeping General Data Protection Regulation (GDPR) on the premise that individuals residing there have the right to control their personal data, and can even request its erasure. Companies possessing the data must respect and protect those rights or face hefty penalties.

Against this backdrop, businesses across industries are investing in professionals whose job it is to mind our data and keep it safe and secure. In this three-part cover story, you will meet some of the many St. John's Law alumni who work in the related fields of data privacy, cybersecurity, and compliance.

KEEPING OUR DATA PRIVATE

Our world is digitizing at breakneck speed. We've adopted the internet faster than any other technology in history, and it's predicted that there will be 27.1 billion networked devices by 2021. With all this connectivity, we're creating and sharing scads of new information every second.

That personal data is the lifeblood of businesses we engage with every day. We entrust it to them, and assume they will use it responsibly. When that data—and our trust in its safety and security—gets breached, there can be major consequences for the individuals and companies affected.

Recognizing the value and vulnerability of our personal data, federal and state entities in the United States and countries around the world have taken steps to regulate how companies collect, use, store, and dispose of it. In turn, companies are investing significant resources in lawyers and other professionals who shape and guide their data privacy strategy and functions.

As vice president, corporate counsel, cyber and privacy law, at the American Fortune Global 500 and Fortune 500 company Prudential Financial, **MARK FABER '84** has had an insider's view of the fast-evolving data privacy field for over a decade.

"Only a handful of people were practicing privacy law 20 years ago," he says. "Yet, recently, the practice has grown exponentially and is now a critical component of virtually every key corporate business initiative. Privacy attorneys advise companies on how to use data in compliance with laws and regulations, how to collect and use personal information for the benefit of customers and consumers in a transparent manner, and how to provide the necessary notices and disclosures, among other responsibilities."

Faber, who previously practiced labor and employment law for many years, finds privacy work interesting and wonderfully rewarding. As advances in technology release more and more of data's potential, he notes, privacy issues become more complex, and the risks associated with keeping data protected grow. "A recent survey found that corporate C-Suite executives overwhelmingly consider the disclosure of personal information as one of the largest threats, if not *the* largest threat, to their companies," he shares. "That indicates how seriously businesses are taking this issue."

Analyzing, and finding solutions to, complex issues is an aspect of his work that Faber particularly enjoys. "At Prudential, I have the opportunity to collaborate with internal business clients at an early stage and provide practical advice to help them meet their goals," he says. Working as a privacy attorney for a global company also presents some unique challenges. "2018 was a landmark year in the privacy world," says Faber. "The GDPR—the most comprehensive privacy law in decades—became effective and applicable to EU entities as well as to any company outside the EU that offers products and services to individuals who reside in the EU." Brazil, Argentina, India, and other countries have also enacted GDPR-like laws.

So far, the United States hasn't followed suit. "The U.S. takes a sectoral approach to privacy, with various federal laws that regulate different areas of privacy," Faber explains. State laws are even more numerous. But the U.S. privacy landscape is changing dramatically because of the recent enactment of California's milestone Consumer Privacy Act of 2018 (CCPA). "The CCPA isn't effective until 2020, but it's the broadest and most impactful privacy law in the country's history," says Faber. "It applies to all California residents, broadly defines personal information, and creates additional notice obligations. It also affords California residents individual rights, including the right to know what information a business collects about them and the right to erase data under certain circumstances."

Examining new and proposed data privacy laws, reviewing them pre-enactment with government affairs and trade associations, and interpreting them after they become law is all part of a good day's work for Faber.

"Privacy law is a great fit for lawyers who want to constantly learn something new, who can tackle complex problems, and who enjoy building client relationships," he says. "It's never boring."

CHRISTINA TSESMELIS '05, an adjunct professor at St. John's Law, echoes Faber's sentiment as she reflects on the five years she spent as senior vice president and global head of anti-money laundering, anti-corruption, and privacy at Neuberger Berman Group, an international investment advisor and broker-dealer. "I provided legal counsel on privacy matters across all lines of business worldwide, drafted and implemented a privacy policy in over 20 countries, and trained employees on that policy," she says. "There was never a dull moment."

Tsesmelis entered the privacy field after clerking for two federal judges in New York and working as a litigator at a major law firm, with a focus on white-collar defense and securities enforcement. It was a timely move. "A decade ago, not every financial services firm had a dedicated privacy officer with a certain level of experience," she says. "But businesses in and beyond the financial sector came to see that protecting and preserving personal data isn't a luxury. It's a critical component of doing business successfully in our digital age. Now, most, if not all, firms have at least one attorney dedicated to privacy at a global level."

Taking a global view, Tsesmelis says, proved critical to her privacy work. "One of the challenges of my role was drafting a privacy policy that protected the firm while being jurisdiction neutral," she shares. "In other words, it had to be flexible enough to apply to all of the firm's lines of business around the world." It was a task that required her deep expertise in the GDPR, similar international laws, and the bramble of U.S. federal and state data privacy mandates.

"I had to ensure that the firm was abiding by the applicable regulations, and I had to anticipate how else to protect the firm, its employees, and clients from possible

events that weren't contemplated by the regulations," Tsesmelis says of the fast-paced role. "I was able to look globally and examine how other nations protect their citizens. In the process, it became clear that sometimes the United States is a leader in the privacy arena, and sometimes its laws fall short by comparison."

Considering her work and how she made her mark in the data privacy field, Tsesmelis says: "To be successful in this area, you need to be able to think not only as a lawyer, but also as a technology professional. The wide variety of classes I took at St. John's Law, the real-world experience I gained in clinics and internships, and the Law School's proximity to the world's financial center enhanced my ability to learn quickly and to wear both a law and a technology hat."

NICOLE OVERSIER '06 agrees that a St. John's legal education provides a strong foundation for a career in privacy law. As senior counsel at the global professional services company Aon, she is a member of the Asia regional legal team supporting the company's risk, health, and data and analytics capabilities across North and Southeast Asia. "My role involves working closely with our privacy team to ensure that Aon's core products and services are compliant with applicable data privacy laws and that wider data privacy risks are effectively managed," Oversier says.

The experience and perspective she brings to the position roots in her earlier work in the Asia capital markets practice of a leading global law firm and in house at companies in India and Singapore. "Almost 13 years and three countries later, I'm still based in the region and still thankful to be able to work in multiple jurisdictions with diverse clients and colleagues," Oversier says. She also appreciates the opportunity to work in an evolving area of the law.

"As our digital universe of data—and its commercialization—continues to grow, the role of data privacy professionals has become incredibly vital, since they're tasked with supporting innovation while mitigating associated legal and reputational risks," she observes. "What I enjoy most about being in the data privacy arena is that it intersects with both technology and law. Plus, as a truly global business, it opens doors for young lawyers to practice across geographical boundaries."

As Oversier sees it, those opportunities will only continue to grow as regulators worldwide look for new ways to protect the data moving across their borders. "Companies are being held accountable, and a lot is being done to reduce risk, but threats to personal data are always present and always evolving," she says.

Also ever-evolving is the concept of privacy itself. "Privacy is one of the most rudimentary building blocks of personhood and, in our complex technological age, personal data is inextricably tied to our privacy," says **MOYA N. BALL '16**, a data privacy attorney with IBM's general counsel and corporate privacy offices. "I have the privilege of playing an important role in maintaining the integrity and assuring the protection of that personal data."

Ball got her start in the privacy field at the multinational health care products and services distributor Henry Schein, Inc. (HSI), where she began working while she was in the evening program at St. John's Law. "Privacy law factored generally into my role at HSI, but it wasn't until I had the opportunity to lead the company's privacy compliance initiative in response to the adoption of the GDPR that I realized I wanted to focus on privacy law," she says. When the opportunity to work at IBM presented, she knew it was the right next step in her legal career.

"I primarily advise IBM's global businesses on transactional matters requiring GDPR expertise, such as mergers and acquisitions, divestitures, and initiatives involving AI, cognitive, and cloud solutions, cognitive health solutions, and various client services," Ball explains. "In supporting AI, cognitive, and cloud solutions, I further assure adherence to 'privacy by design' principles that require the integration of data protection early in the development of technology solutions. I also support the company's business and legal teams in negotiating GDPR data processing agreements with some of IBM's largest clients, and I advise the organization's cybersecurity teams in compliance with U.S. data breach laws."

Her work at IBM, Ball says, draws on the critical thinking, analytical reasoning, and clear communication skills she honed at St. John's Law. "St. John's also provided exposure to novel areas of law in a practical manner, and with this academic experience I felt confident in my ability to step into such a demanding role," she adds.

As she guides IBM, Ball weighs how the concept of privacy, its application to data, and the related legal framework are bound to change. "Particularly in the United States, we need a cultural shift in how we view our personal data," she says. "We often share it out of convenience and not necessity, sometimes unknowingly, and with little thought to privacy consequences. For the law to keep pace, we all need to keep pace. It's a global call to action, and a tremendous opportunity for present and future privacy attorneys to help protect data as a precious resource."


MARK FABER


CHRISTINA TSESMELIS


NICOLE OVERSIER


MOYA N. BALL


PAUL FERRILLO


LEO TADDEO


JUDITH H. GERMANO


JOSEPH V. MORENO

KEEPING OUR DATA SECURE

With the rise of our digital economy, cybercrime has become a very lucrative industry. It's reported that hundreds of billions of dollars have been lost to data breaches perpetrated by nation state hackers, crime syndicates, and individual bad actors in recent years. The threat is so high that the U.S. Treasury Department has designated cyberattacks one of the greatest risks that America's financial sector faces.

To mitigate and manage that risk, financial services companies and businesses across industries tap the niche expertise of cybersecurity professionals. Cybersecurity is about protecting data in its electronic form, and elemental to that protection is knowing what the critical data is, where it resides, and how to defend it from unauthorized access.

As more people bring their lives online and expose their personal data to theft, misuse, and human error, the work of lawyers in the cybersecurity field is becoming increasingly essential to the safety and wellbeing of the global citizenry and marketplace.

PAUL FERRILLO '86CBA, '89L, a shareholder at Greenberg Traurig LLP, brings a wealth of experience to his work in the firm's cybersecurity, privacy, and crisis management practice. "Taking a partnership at Greenberg Traurig is the pinnacle of my long career in corporate governance, corporate investigations, and corporate litigation, advising directors and officers in areas of risk in both pre- and post-litigation situations," he says. "Every job was a stepping stone to the next."

While Ferrillo enjoys helping clients navigate the increasingly difficult risk and regulatory environment to stay "cyber safe and secure," he concedes that the practice has its challenges. "Cybersecurity is one of the fastest-paced areas of the law, litigation, and corporate governance that I've ever experienced," he says. "It seems to change every three to six months, and requires constant learning about new regulations, cases, and solutions." Then there are the ever-looming, and ever-changing, threats. "An expression I hear and use a lot is: 'Somebody is trying to hack you right now, as we're speaking. Are you prepared?'," Ferrillo says. "Many companies simply aren't, and I suspect the problem might be getting worse."

To put the practice area's dynamic nature in even sharper perspective, Ferrillo notes that the regulatory effort around cybersecurity "is really the new kid on the block." It's been just five years since the National Institute of Standards and Technology introduced its seminal cybersecurity framework. Two finance industry regulators, the SEC and FINRA, followed with comprehensive cybersecurity guidance, and then a number of states established their own requirements. Finally, the EU's GDPR, California's CCPA, and sweeping mandates out of the New York State Department of Financial Services set a new and higher bar for regulating cybersecurity. Disclosure to regulators, once relatively rare, is now the rule.

Working with competing cybersecurity regulations isn't for the timid, Ferrillo says, but it's a good fit for lawyers who have multiple skill sets and who like to solve complex problems that combine regulation, investigation, and potential civil litigation at the same time. "I recently had one breach with hundreds of back doors that gave the attacker access to a network," he shares. "Those doors needed to be methodically found and closed." To do that, Ferrillo says, he drew on knowledge and skills he gained at St. John's Law.

"The late Professor David Siegel, who I dearly adored, taught me all about New York State and Federal practice," he recalls. "Through St. John's moot court program, I learned to think and speak on my feet, and to write a good, succinct, and pointed legal brief. Indeed, all of my professors taught me and my classmates to be thorough, effective,

and holistic lawyers—skills that I keep in my toolbox today to help clients deal with intricate problems."

Like Ferrillo, **LEO TADDEO '94** believes that his St. John's legal education prepared him well for a career in cybersecurity that began during his 20-year tenure with the FBI. "St. John's sharpened my ability to analyze and solve complex problems," he says. "While I always knew the value of personal ethics, fairness, and justice, I learned how to advocate for those principles as a law student. These skills have been critically important to me in my professional and personal life."

Taddeo, a U.S. military veteran, began his legal career as a criminal investigator with the FBI in New York, and then assumed a succession of senior roles with greater responsibility for FBI operations around the world. "Like just about every other FBI agent, I wanted to work the biggest, hardest, and most impactful investigations," he says. "For the majority of my years as an agent, that meant organized crime, white collar crime, and terrorism cases. It wasn't until late in my FBI career that I recognized the importance of cybercrime and gravitated toward assignments in that field. Given that there weren't many senior executives with cyber expertise in the FBI, I soon found myself in a small group of experienced investigators who could effectively supervise cyber programs."

Eventually, Taddeo left the FBI and took his cybersecurity expertise to the private sector, where he now serves as chief information security officer at Cyxtera Technologies. "My primary responsibility is to ensure the security of the critical information assets that Cyxtera depends on to do business," he explains. "This includes general IT security, compliance, and product security. I also work with Cyxtera's developers to improve the features and capabilities of the security products we offer to our customers."

Considering the state of his field today, Taddeo notes that, out of sheer necessity, financial services companies lead every other sector in developing and deploying cybersecurity controls. "This lead is the result of investments in staff and security tools internally and external, cross-sector collaboration," he says. "By sharing and cooperating with each other, financial institutions make the entire sector more secure and resilient."

Innovation, Taddeo points out, is fueling this effort. "Companies are investing heavily in machine learning and artificial intelligence that can predict malicious activity and take action," he says. "And they're setting up analytics and information 'fusion centers' that find and combine all of the information sources available to the enterprise to create a threat picture that enables the institution to better understand its risk profile and more efficiently respond to incidents."

While innovation is key to preventing, combatting, and recovering from cyberattacks, **JUDITH H. GERMANO '96** recognizes that many cybercrimes are still relatively unsophisticated. "Malware attacks launched through phishing emails and similar low-tech schemes remain prevalent" she explains. "And they can be prevented by low-cost measures, such as using two-factor authentication, limiting data access, keeping software updated, and requiring complex, unique passwords or other access credentials."

Cybersecurity is a focus of Germano's work as principal of Germano Law LLC. "I was a federal prosecutor for 11 years before starting my own boutique firm," she shares. "As chief of economic crimes at the U.S. Attorney's Office for the District of New Jersey, I was involved in, and supervised, cybercrime investigations and prosecutions, among other responsibilities. I saw how cyberthreats were growing, and that companies needed help handling them."

Germano also traces her interest in cybersecurity back to her time at St. John's Law. "I wanted to earn a law degree so I could guide organizations and executives through crisis," she says. As the research and symposium editor of the *St. John's Journal of Legal Commentary*—now the *Journal of Civil Rights and Economic Development*—I coordinated a symposium on Cyberspace and the Law. It was one of the very first conferences of its kind, and it introduced me to the field of cybersecurity in all its complexities."

In addition to working as a cybersecurity attorney, Germano engages her expertise as a distinguished fellow at the NYU Center for Cybersecurity, as a senior fellow at NYU's Reiss Center on Law and Security, and as an adjunct professor at NYU Law. "Good cybersecurity starts with a risk assessment that focuses on the systems and data an organization has, who has access to them, how they're protected, and what threats they face," she shares. "I enjoy helping executives and officials develop and test systems, plans, policies, and procedures for improving cybersecurity in their organizations. I'm dealing with critically important issues at the intersection of security, technology, and business. It's fascinating and rewarding work."

JOSEPH V. MORENO '99L, '00MBA agrees that it's very gratifying to be a trusted cybersecurity advisor. He handles a range of matters related to data protection and incidents as a partner in the white collar defense and investigations group at Cadwalader, Wickersham & Taft LLP.

"Having worked for years with corporate clients across industries in developing and implementing anti-bribery and anti-money laundering programs, cybersecurity was the next logical space to develop as a practice area," he says. Moreno's practice in this niche is also informed by his earlier career in the U.S. military, as a national security prosecutor with the U.S. Department of Justice, and as a consultant to the FBI's 9/11 Review Commission. "In these diverse roles, I gained subject matter expertise in dealing with cyberterrorism conducted by hostile foreign actors," he shares.

His broad base of experience affords Moreno a clear view of the current threat landscape. "The danger of being hacked was bad enough when we were dealing solely with lone wolf attackers," he says. "Now we have sophisticated, foreign military and intelligence-backed hacking operations supported by the likes of China, Iran, Russia, and North Korea who act with impunity." These ever-growing threats—and constantly developing cyber regimes like the EU's GDPR and regulations enacted by California, New York, and other U.S. states—only add to the potent cybersecurity mix that, Moreno says, makes these challenging times for companies.

Given these challenges, seasoned cybersecurity lawyers have become essential to corporate wellbeing. "We're there to advise clients on regulatory, litigation, and public relations matters, and that can go a long way to addressing the merits of a cybersecurity breach while also restoring public confidence," Moreno says. "How you handle yourself in the first few hours following a breach can mean the difference between a temporary dustup and a long-term disaster."

As he weighs what it takes to succeed as a cybersecurity attorney, Moreno is clear that St. John's Law graduates are up to the task. "St. John's lawyers are practical and know how to handle themselves in the courtroom, the boardroom, or in front of the media," he says. "We are deliberative and thoughtful, but also know how to make judgment calls and shift gears when faced with fast-changing events. Lawyers are generally well trained to handle crisis response, but St. John's lawyers are especially well suited when it comes to reacting under fire to achieve the best results for our clients."

KEEPING COMPANIES

Data privacy and cybersecurity regulation didn't start with the 2008 recession in the United States, but the crisis certainly put regulatory watchdogs into overdrive across the financial sector. America is now home to a maze of federal and state rules and requirements around data protection. And the EU's GDPR is one of the most stringent and far-reaching efforts to date.

Any company or individual that processes personal data is responsible for its protection and, by extension, can be held accountable for a data breach under the GDPR. Since international financial services firms typically hold huge amounts of personal data, this regulatory scheme is having an outsized impact on them, their vendors, and other third parties they work with. Penalties for non-compliance can be steep, with companies facing fines of up to four percent of their annual global turnover.

With this regulatory thicket to navigate, firms are building out their compliance operations and, increasingly, hiring lawyers to lead and advise them. Working in house or as outside counsel, these professionals support the company's business areas in their duty to comply with external regulations. They also devise, implement, and monitor internal systems that ensure the company's compliance with external mandates.

As a partner at Cullen and Dykman LLP, **KEVIN PATTERSON '81C, '83MBA, '86L** focuses his work on bank operations and compliance, particularly in regard to the online and mobile delivery of financial services. It's a dynamic practice that taps the knowledge and skills he gained over a career that started at Cullen and Dykman and then took him in house at a succession of major financial services firms, where he provided legal counsel on client matters at the intersection of technology and business.

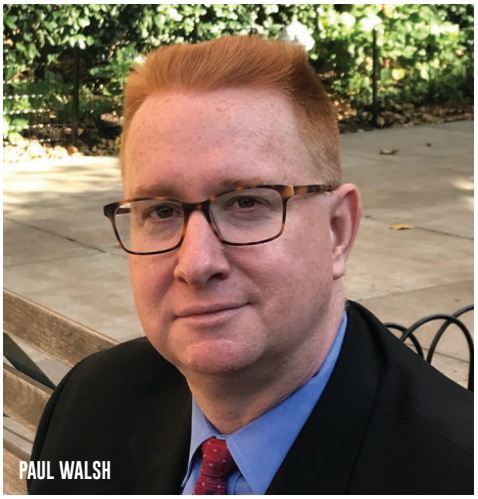
"I've been back at Cullen and Dykman for more than five years, and the variety and depth of my experiences as in-house counsel have been invaluable as I advise clients on regulatory compliance," Patterson says. He particularly enjoys the wide variety of matters he handles. "Our clients are always looking to introduce new products and services, and come to us with a host of interesting compliance and legal issues," he shares. "Enhancing mobile banking features is a current focus, for example. At the same time, the relevant regulations are continually growing and changing. That keeps things interesting and never too routine."

More than 30 years along his professional path, Patterson can still see the connecting points to his St. John's legal education. "Compliance professionals with a legal skillset deliver benefits to an organization," he says. "They have an enhanced ability to take a regulation and break it down to its component parts to better understand its intended purpose and practical impact. St. John's Law teaches students how to perform and synthesize legal research and translate those actions into meaningful legal services. It also instills a pragmatism that serves lawyers well as they undertake the detail-oriented analysis required to work in compliance successfully."

PAUL R. WALSH '92, who is an adjunct professor at St. John's Law, makes a similar connection between his Law School education and his role as the head of compliance and regulatory risk for Commonwealth Bank of Australia (CBA) in the United States. "Much of my work today is advisory in nature," he says. "I'm asked to give an opinion based on the regulations and my experience and, each time I do, I need to be prepared to 'make the case' for my view and communicate it clearly. My legal training at St. John's provided a solid foundation for this advisory role."

After graduating from St. John's, Walsh worked as a trial lawyer. "The skills I used to build cogent and persuasive arguments in the courtroom translated well to a career helping companies manage risk and comply with regulations while they innovate to make their businesses profitable," he notes. Over the years, Walsh has employed those skills and others while leading compliance operations at prominent financial firms, including JPMorgan Chase, TD, Betterment and, now, CBA.


KEVIN PATTERSON


PAUL WALSH

"I enjoy collaborating with my internal clients to find right-fit options for conducting their business in a regulatory compliant manner," he says. "Working through complex problems and explaining the reasoning along the way, you can develop action plans beyond a simple 'no this can't be done.' This is where a proactive compliance professional adds true value without compromising the core 'do the right thing' tenet that every company should operate under."

As **PETER E. PISAPIA '94CBA, '97L** sees it, lawyers who work in compliance also add tremendous value by helping companies keep up with ever-changing data protection regulations. "One of the biggest challenges with respect to data

IN COMPLIANCE


PETER E. PISAPIA


RUTH CALAMAN

privacy and cybersecurity is the whirlwind of technological advancement," he says. "Compliance professionals have to stay up to date on the latest practices and capabilities. As Wayne Gretzky said about playing hockey—you have to be where the puck is going, not where it's been."

The analogy plays out for Pisapia in his position as senior director at TIAA and chief compliance officer of the TIAA Life Insurance Separate Accounts. "I head the compliance program for the TIAA and CREF registered funds complex," he explains. "My primary responsibilities include managing a team to assess regulatory risks and to develop and maintain policies, procedures, and monitoring activities. We also interact with federal and state regulators and provide compliance training to employees and personnel."

Pisapia started in compliance after an early career as an in-house mutual funds attorney. "I was probably the only student at St. John's Law who knew from my first day that I wanted to be a mutual funds lawyer," he shares. "But I didn't consider compliance until after I had practiced for a few years." Pisapia is happy he made the switch, and finds his current work particularly rewarding.

"TIAA is a large organization with many business lines and industry-leading practices," he says. "We also are the fiduciary to millions of wage earners who entrust us with their retirement accounts. My team is here to keep their assets and data safe." It's a big job that benefits from legal training, says Pisapia. "The ability to analyze and understand complex securities laws and regulations, problem-solve, and write and communicate well—all skills you can hone at St. John's Law—are excellent qualifications for compliance officers."

RUTH CALAMAN '97 agrees that compliance work is an excellent fit for lawyers generally, and for St. John's lawyers in particular. "The work challenges you every day to apply the rule of law to real-life situations," she says. "It's not about theory and abstract principles. As a compliance professional, you're called upon frequently to determine whether a particular action or decision is compliant, or if it would violate a law, regulation, policy, or procedure. To make that determination, you need to be able to view the facts and circumstances objectively and consider established guidelines for the action or decision in question."

Calaman relied on the knowledge and skills she acquired at St. John's as she charted an impressive career path in senior finance industry legal and compliance roles. Today, she serves as chief compliance officer and general counsel of Evercore Wealth Management and Evercore Trust Company, N.A. "As CCO, I'm responsible for all aspects of the compliance program," she says. "I ensure the businesses are up to date with regulatory requirements and that they respond to regulatory changes as they occur by updating their policies, procedures, and practices. I also manage regulatory examinations and inquiries, and ensure that regulatory filings are accurate and timely."

The role puts Calaman on the frontlines of data protection. "I spend a lot of time training our employees about client data confidentiality and safety, and about the dangers involved in misusing that data," she says. "I also work closely with our IT team to ensure that our client data is secure from unauthorized access." This crucial compliance work can get complicated, but Calaman rises to the challenge.

"When there's a potential issue at a global company that involves multiple clients and vendors, figuring out whether you have a reportable matter takes time and attention to detail," she says. "There is no single, national or international standard to follow, so compliance professionals have to be familiar with the tangle of rules and regulations for data privacy and security, including rules that apply in places where the business is located, where the client resides, and where the vendor is present. Each jurisdiction has its own standards, requirements, and definitions, so what may be problematic in one place may not necessarily be an issue in another."

A different challenge for compliance leaders, says **EUGENIE (GENIE) CESAR-FABIAN '04**, is bridging the divide between how junior and senior professionals in a company understand and use technology. But with that challenge comes opportunity that Cesar-Fabian seizes as general counsel and chief compliance officer at Palladium Equity Partners, LLC.

"Since the majority of senior executives in financial services built their careers when cell phones and email were technological novelties, it can be hard to translate where to draw the line between the need to protect the electronic data we use and the need to access that data quickly and effectively so the firm can meet its business objectives," Cesar-Fabian explains. Mediating between these competing needs is the perfect job for a

compliance leader who is well versed in law and technology.

"If a CCO has a good understanding of where the business line wants to go with respect to technology, can identify the potential pitfalls to the firm, and can speak to the relevant issues with both tech-savvy junior professionals and senior professionals aiming to unlock efficiencies, then he or she can help inform the decision-making process to find the best possible path forward," Cesar-Fabian says. "Say the firm is like a high-performance race car. Compliance professionals want to serve as a solid braking system that can help protect it from serious accidents, without necessarily erecting walls in front of it."

Cesar-Fabian took the in-house legal and compliance job at Palladium following a career in private practice at major law firms. "When I first joined Palladium, I worked with senior management to build out and implement a robust regulatory compliance program, from drafting the written policies and training employees, to implementing an efficient way to track and monitor the program," she says. "Since then, it's been my job to monitor, maintain, and update the program as we've continued to grow and thrive as a firm."

With that growth and success, Palladium has expanded its legal and compliance operation, welcoming Cesar-Fabian's St. John's Law classmate and friend, **DOMINICK BARBIERI '04**, to the team two years ago as associate general counsel and deputy chief compliance officer. "Dom and I were close in law school, and were two of three in our study group from our first year through graduation, so you can imagine how elated I was when we were able to bring him in," Cesar-Fabian says. "We weren't just getting an exceptionally intelligent, talented lawyer, but someone I knew and trusted from the start."

The feeling is mutual for Barbieri, who held a federal clerkship just out of St. John's and then practiced as a big firm litigator before joining the SEC's Division of Enforcement. "Palladium has been one of the best professional experiences of my life," he shares. "Transitioning from a litigation and government enforcement perspective to an in-house role at a middle-market private equity firm is a significant change in the day-to-day demands of the job and culture. Being able to bounce things off a friend and colleague has been wonderful, and I've benefitted immensely from Genie's mentorship."

His role at Palladium, Barbieri says, is a natural fusion of the skills he learned as a government lawyer, in private practice, and at the Law School. "The number one skill I employ daily is critical thinking," he says. "Being able to approach complex problems in a methodical way has been key to my professional achievements. I also use the 'soft skill' of emotional intelligence regularly. It's invaluable when offering real-world advice as a lawyer and compliance officer to help my firm achieve its goals and protect the data it's entrusted with."

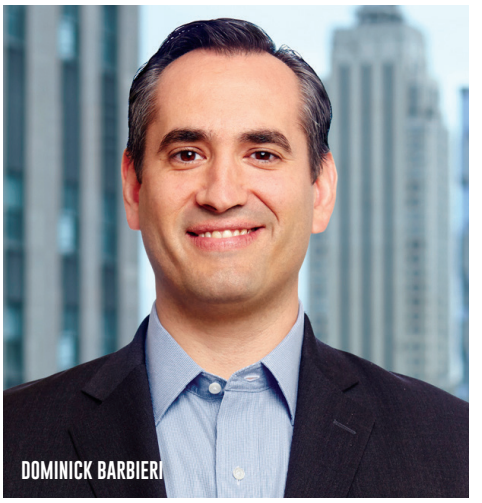
SABEENA AHMED LICONTE '06, the chief legal officer and chief compliance officer at Bank of China International (USA) Holding Inc. (BOCI), also draws on skills and experience she gained at St. John's Law. "During my 2L year, I had an internship in the Regulatory Compliance Department at Merrill Lynch," she says. "We started our weekly meetings by slapping the *Wall Street Journal* and *New York Times* down on our conference table to see which financial services firm had made it to the front page because of some alleged wrongdoing. That's how I learned all about reputational risk and how it interplays with a company's wellbeing."

As a 3L, Liconte amassed more real-world experience working in the securities fraud prosecution division at the New Jersey Attorney General's Office. With that practical insight, after graduation, she started her career in the legal division of Bank of New York Mellon. Moving in house at a start-up futures broker, Liconte was tapped to serve as the firm's general counsel and chief employment officer. She then went to E*Trade Financial Inc. before starting at BOCI.

Liconte relishes the opportunity to work in a field that is always evolving. "I started out as electronic trading was dramatically changing the finance industry," she says. "Today, we're seeing similar shifts with the rise of virtual assets, like cryptocurrencies and bitcoin, and with more of the world's transactions occurring online in real time." As the digital economy matures, Liconte sees the work of lawyers in the compliance field expanding.

"We're the in-house experts on how companies can grow and prosper while meeting their obligation to safeguard the personal data they collect, use, and share," she says. "As that data pool gets bigger and becomes an even more valuable corporate asset and global currency, the regulatory framework will naturally change to keep pace. This constant change is what keeps compliance work so interesting, and makes it such an exciting time to be in the field."


EUGENIE CESAR-FABIAN


DOMINICK BARBIERI


SABEENA AHMED LICONTE

ST. JOHN'S UNIVERSITY
SCHOOL OF LAW
8000 UTOPIA PARKWAY
QUEENS, NY 11439

WHY I GIVE BACK

"The Ronald H. Brown full-tuition scholarship was instrumental in allowing me to realize my lifelong dream of becoming an attorney. I'm now building a rewarding career at a top-tier law firm and I'm able to effectively give back to my community. This scholarship validated my hard work and encouraged me to aim for excellence. I remain grateful to St. John's Law and to our generous alumni for this opportunity."

— Janelle Johnson '16
Associate, WilmerHale

PLEASE SUPPORT SCHOLARSHIPS AT ST. JOHN'S LAW. USE THE ENCLOSED ENVELOPE TO MAKE YOUR GIFT, OR GIVE ONLINE AT STJOHNS.EDU/LAW-GIVING