WWW.AMERICANBAR.ORG/INTLAW

# INTERNATIONAL LAW NEWS

FALL 2017 VOL. 46 NO. 1

SECTION OF INTERNATIONAL LAW AMERICAN BAR ASSOCIATION

## Managing Big Data Privacy and Security

By Aliya Ramji, Deniz Tamer, Carina Barrera Cota, Renato Leite Monteiro, Caio César C. Lima, Joseph Prestia, and Kristina Subbotina

Companies are inundated by big data on a daily basis. Big data is a term that describes large volumes of data, both structured and unstructured. Some companies use data in its anonymized and aggregate form, while others use identifying information for targeting. Social media companies, for example, collect more than just a username and images. They can collect data on everything from time of use, duration of session, demographics, interests, frequency of use, geolocation, and more. This trend toward more data will only continue to accelerate with the transformative growth and ubiquity of connected technologies such as cloud services, connected cars, smart cities, the Internet of Things, and other breakthrough innovations. But it's not the amount of data that's important; it's what organizations do with the data that matters. Big data can be analyzed and mined for insights that lead to better decision making and strategic business moves. Data mining may expand business opportunities and customized services, but it also can trigger legal, regulatory, and public-relations pitfalls for the unwary.

With all that data, implementation of data security and privacy safeguards is becoming more and more important in a

*continued on page 4*

# CHAIR'S COLUMN

## A World of Programming Ahead

**Steven M. Richman** (*srichman@clarkhill.com*) **is a partner at Clark Hill PLC, where he practices domestic and international commercial law, and is Chair of the ABA Section of International Law 2017–2018.**

This issue of the Section's *International Law News* features articles on big data privacy and security and on the internationalization of law firms. The emphasis in these articles on pragmatism in dealing with privacy, cybersecurity, law firm management, and growing referrals is timely and necessary. As an additional overlay to the increasing use of technology in global practice, we have the added element of artificial intelligence. The overriding lessons, drawn from the front pages, are that no one and no company is immune, and that the technology will continue to expand, improve, and become more pervasive. The question is how we adjust, adapt, and, where appropriate, regulate. At our Spring Conference in New York in April 2018, we will have an entire track devoted to these issues.

Many other initiatives are in the works. The following should give you a feel for the breadth of our programming, projects, and publication activities this year.

Our Fall Conference in Miami during October 24–28 at the JW Marriott in the downtown Brickell area will have a focus on doing business in the Americas, with perspectives and substantive content provided from all regions of the world. The theme is "Doing Business in the Americas in the New Global Economy: A New Dawn in the Hemisphere." These panels will feature speakers from around the world on a variety of topics. In addition, several ethics credit programs will help keep you current and focused on professional excellence. We are also excited to hear from our exceptional luncheon speakers, Ana Salas Siegel, General Counsel, NBCUniversal Telemundo Enterprises; Luis Almagro, Secretary General, Organization of American States; and President Julio Frenk, University of Miami. On Wednesday morning, we are excited to hear welcome remarks from Carlos A. Giménez, Mayor of Miami-Dade County. We will also recognize UN Day on October 24 during the conference.

Planning for our specialty conferences this year is proceeding. We will be in Singapore next May for a day and a half conference on international arbitration, in Indonesia for an ILEX trip in May, and in Copenhagen next June for a day and a half conference on life sciences. We have been working to reschedule our Africa Forum. We are also working on our 2018 Spring Conference in New York. We have taken an innovative approach to organizing programs to balance between traditional business/finance and dispute resolution topics and other areas that include and transcend those topics. For example, we will have a special track of programming on international family law and another on cyber and artificial intelligence issues. The theme for the New York conference is the fusion of public and private law, and we will be continuing our focus on corporate social responsibility. Other activities include continued outreach to the Caribbean Basin and the Baltic states. Our program in San Juan, Puerto Rico, was postponed due to the devastation on the island from the hurricane, but we are rescheduling it for next year. ◆

INTERNATIONAL LAW NEWS
WWW.AMERICANBAR.ORG/INTLAW



*International Law News* (*ILN*) (ISSN 047-0813) is published quarterly by the American Bar Association's Section of International Law, 1050 Connecticut Ave. N.W., Suite 400, Washington, D.C. 20036. *ILN* keeps Section members informed about current international law developments and important Section news. It provides comprehensive legal analysis of international law topics, as well as concrete, how-to advice for practitioners.

*ILN* content represents the opinions of the authors or the Section editors and should not be construed to be those of the ABA or Section unless adopted pursuant to the Association bylaws. Nothing contained herein is to be considered legal advice for specific cases; readers are responsible for obtaining such advice from their own legal counsel. The materials herein are intended for educational and informational purposes only.



*ILN* is available at https://www.americanbar.org/publications/international_law_news to members of the ABA Section of International Law and to subscribers. Send address corrections to ABA Service Center, 321 N. Clark Street, Chicago, IL 60654-7598, service@americanbar.org. Subscriptions are free to Section members. To order nonmember subscriptions ($25), email orders@americanbar.org or call 800/285-2221.

To submit an article, consult *ILN* Coordinating Editor Lori Lyons, ILNquestions@gmail.com, or download the *ILN* Author Guidelines via https://www.americanbar.org/publications/ international_law_news. Send your manuscript for *ILN* Editorial Board review by emailing it as a Word document attachment to ILNquestions@gmail.com.

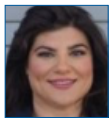
# CONTENTS

## DATA IN THE DIGITAL AGE

# Big Data

*continued from page 1*


**Aliya Ramji** (*aramji@figure1.com*) is the director of Legal and Business Strategy at Figure1 in Toronto, Canada, and is a vice chair of the Section's International Corporate Counsel Committee.



**Deniz Tamer** (*deniz@mticranes.com*) is COO and general counsel of MTICC in New York City and is co-chair of the Section's International Corporate Counsel Committee, a deputy to the chair, and vice chair of the New Member and Law Student Outreach Committee.

**Carina Barrera Cota** (*carina.barrera@mx.ey.com*) is a partner in EY Legal Services, heading the Intellectual Property and Data Privacy sub-practice in EY México, based in Mexico City. Her focus areas are intellectual property and personal data protection.

**Renato Leite Monteiro** is a legal consultant, specializing in privacy and data protection, with Baptista Luz Advogados in São Paulo, Brazil, and is a professor at Fundação Getúlio Vargas, where he teaches intellectual property and cyber law. He is a Certified Information Privacy Professional/Europe (CIPP/E).

**Caio César C. Lima** is an attorney, with a focus on cyberlaw, privacy, and data protection, at Opice Blum Advogados Associados in São Paulo, Brazil, and is a professor at Faculdade de Informática e Administração Paulista (FIAP). He is certified in Privacy and Data Protection Foundation by EXIN.

**Joseph Prestia** is the owner of the Law Office of Joseph D. Prestia, PLLC in Knoxville, Tennessee. He is vice chair of the Section's Privacy, Cybersecurity, and Digital Rights Committee.

**Kristina Subbotina** is counsel, Legal and Business Affairs at an international technology company in Los Angeles, California. She is vice chair of the Section's International Corporate Counsel Committee and vice chair of the International Financial Products Services Committee.


variety of industries. Most companies are now data collectors and are working on protecting consumer data. Companies are also wading in a minefield of legal and technological challenges to effective security and privacy. How do big data businesses and their lawyers deal with the challenges?

At the Fall Conference in Miami, the International Corporate Counsel Committee will sponsor a panel discussion of the legal and corporate considerations for effective security and privacy in the digital era of big data in select countries around the world. The panel will explore the essential role that attorneys and in-house counsel play in helping clients and companies manage the challenges of big data. This article, authored by the program co-chairs and panelists, provides highlights of what will be discussed during our panel, including pragmatic tips for practitioners in Canada, the European Union, the Philippines, Mexico, and Brazil.

## Canada

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) limits the use of personal information to the purpose for which it was collected. "Personal information" is defined broadly and includes any information about an identifiable individual, other than basic information about employees of an organization. Individuals have a right to access personal information held by an organization. The law allows for implied consent depending on the sensitivity of the information being collected. A key question is whether notices are clear enough such that data mining can be reasonably anticipated by users based on a privacy notice. The Digital Privacy Act (DPA) adds the additional requirement that the individual needs to understand the nature, purpose, and consequences of the collection, use, or disclosure of that information.

The DPA also introduced mandatory reporting at the federal level in Canada. The Privacy Commissioner must be notified of any breach that creates a real risk of significant harm to an individual. The definition of significant harm is broad and includes bodily harm, humiliation, and damage to reputation, as well as identity theft and financial loss, among others. The breach must be reported "as soon as feasible"; however, the appropriate amount of time has not yet been determined. Individuals must also be notified if there is a real risk of significant harm from the breach. The notification must allow the person to understand how they will be impacted by a breach and the potential steps that they can take to reduce their harm/mitigate

the risks. Finally, the DPA introduced fines of up to $100,000 for failure to report a breach to the Privacy Commissioner or the impacted individual as soon as feasible.

Lawyers can find ongoing specific examples and guidance on the practical implementation of PIPEDA by businesses from the Office of the Privacy Commissioner (OPC), which publishes findings from compliance investigations. In one investigation of potential misuse of personal information by a business, the OPC found that no consent is required for using publicly available personal information when it is matched with geographically specific demographic statistics. *See* Case #2009-004, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-004. In a case involving social networking sites, the OPC concluded that individuals have a responsibility to read and understand information made available by organizations concerning the use of their personal information. However, businesses must obtain meaningful consent from individuals by providing clear and understandable information about how that organization is using an individual's personal information, including when introducing new digital features. *See* Case #2011-006, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-006. Businesses also must not transmit sensitive personal information through plain-text and unencrypted channels and should take steps to prevent unsolicited and fake ads. *See* Case #2017-002, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2017/pipeda-2017-002.

## Big Data in Healthcare

Public release of health data requires among the most stringent deidentification measures. Because the data can give key insight into a person, his or her preferences, and even private life, in order to protect personal privacy, data is often deidentified, anonymized, or aggregated when analyzed. In healthcare, for example, aggregate data is used to develop information about groups of patients. It allows healthcare professionals to identify common characteristics that might predict the course of the disease or provide information about the most effective way to treat a disease. It is often used for disease prevention purposes.

While useful, the personal privacy of individual patients should not be compromised in the process. Under the guidance of the Information and Privacy commissioner of Ontario (Canada's most populous province), deidentification is a crucial tool in the protection of privacy. Deidentification, combined with simultaneous reidentification risk measurement procedures, is a valuable and effective tool in the protection of personal privacy. This is similar to the practice in the United States. Section 164.514(a) of the HIPAA Privacy Rule provides the standard for deidentification of protected health information. Personal health information is not individually identifiable if it does not identify an individual. HIPAA enumerates eighteen key identifiers that need to be removed from a patient file, case, or image for it to be considered deidentified.

## Canada | Tips for Practitioners

- Limit collection and retention of personal information, especially personal information such as personal health information and financial information.
- Clear, simple language should be used when requesting consent, particularly when dealing with vulnerable populations.
- Have a privacy policy and explain the types of information that are being collected.
- If your company does experience a data breach, report it to the Privacy Commissioner and the affected individuals as soon as feasible.

## European Union

The General Data Protection Regulation (GDPR), which enters into effect on May 25, 2018, modernizes and establishes new requirements related to data privacy, safeguards against data breaches, and the processing, usage, erasure, and portability of personal data. *See* EU Commission Regulation, 2016/679, 2016 O.J. (L 119). Personal data is considered any information related to an identified or identifiable natural person. An identifiable natural person means that the person can be directly or indirectly identified by one or more characteristics, including by an identifier, location, or characteristic, such as physical, physiological, genetic, mental, economic, cultural, or social identity.

Many companies, including cloud-based providers and those who use them as part of their business practices, will be impacted by these new rules. The regulation applies to the processing of data by controllers or processors in the European Union, whether or not the processing actually takes place in the EU. The regulation also applies to the processing of data by controllers or processors when it involves a person located in the EU and the activities are related to the offering of goods or services, even if free, to persons in the EU or the monitoring of their behavior within the EU.

Ultimately, personal data must be processed "lawfully, fairly and in a transparent manner" under Article 5(1). This means that information should be collected for a specific purpose,

that only the information necessary to realize that purpose should be collected, that the information should be accurate and, if necessary, up-to-date, that information should be processed in a way that "ensures appropriate security," and that information should be retained for no longer than is necessary.

"Processing" data, under Article 4(2), is any operation or set of operations performed on the data, whether or not it is done by automated means. Per Article 6(1), processing is lawful if it is: undertaken with the consent of the data subject; is necessary for the performance of a contract to which the data subject is a party; is necessary to satisfy or to comply with a legal obligation; is necessary to perform a task carried out in the public interest or in the exercise of official authority; or is necessary "for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject… in particular where the data subject is a child."

Consent must be ". . . any *freely given*, *specific*, *informed* and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Article 4(11) (emphasis added).

Generally, the processing of personal data revealing racial/ethnic origin; political, religious or philosophical beliefs; health or genetic data; "biometric data for the purpose of uniquely identifying a natural person"; or data about an individual's sexual orientation or sex life is prohibited under Article 9(1). There are specific exceptions to the general rule, as given in Article 9(2)(a), including where the data subject has provided explicit consent for the processing of that personal data, unless Member State law disallows the possibility of giving that consent.

An individual has the right to object at any time to the processing of his or her personal data, including data profiling for direct marketing. Companies that continue to send direct marketing to the individual after the person objects could face financial penalties. The individual does not have an absolute right to object to data processing, however. Article 21(6) contains exemptions for scientific, historical, and health research, for statistical purposes, and for the legitimate interests of the controller or third party. The individual also may not be able to restrict data processing and profiling when in the public interest, as needed for legal claims, or as needed to protect the rights of another person.

The "transparency" goal of the GDPR is especially conspicuous on the subjects of automatic individual decision making and profiling. Article 22 defines automated individual decision-making as ". . . a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Profiling, defined in Article 4(4), is a form of automated processing of personal data in order to analyze or predict an individual's interests or preferences, traits (including health), economic situation, work performance, location or movements, and reliability.

The individual has the right not to be subject to a decision based solely on automated processing, under Article 22. However, this does not apply if the application of automated decision-making is necessary for the performance of a contract between an individual and the data controller, if authorized by EU or Member State law to which the controller is subject, and "which also lays down suitable measures to safeguard the individual's rights and freedoms and legitimate interests," or is based on the subject's explicit consent, according to Article 22(2). Because this consent must be informed, the data subject must be informed about the decision-making logic used and any foreseeable consequences she or he may experience as a result of the processing, whether or not personal data is collected from the individual (Articles 13(2)(f), 14(2)(g), 15(1)(h)). Additionally, automated decisions shall not be based on any of the categories identified in Article 9, as described above, unless "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place" and carried out to further a "substantial public interest" or with the data subject's explicit consent, pursuant to Article 22(4).

Article 22(3) also specifically enumerates the individual's right to have "human intervention" in the decision-making process to protest the decision or to express his or her perspective. It is also worth noting that Article 68 establishes the European Data Protection Board as the successor to the European Data Protection Supervisor (EDPS). Among its responsibilities, as given in Article 70, is issuing guidelines, recommendations, and best practices, including providing criteria and conditions for profiling and automated individual decision-making.

To further the lawful, innovative uses of big data, the GDPR permits data controllers to use privacy-enabling deidentification techniques, such as the substitution of some of an individual's personal data with a reversible value to achieve pseudonymisation. Under Article 4(5), the reversible value's "key" and other information that can reidentify the data subjects must be kept separately from the pseudonymized information and is subject to "technical and organizational" safeguards to prevent reidentification.

There is, however, an inherent risk of reidentification of pseudonymized data. This can happen through the theft of the key that links the pseudonymized with data subjects' identities or by combining "indirect identifiers" (i.e., information

that, in isolation, does not identify the data subject) in the dataset with each other or with other information. It is ultimately the data controller's responsibility to use "appropriate and effective measures" to protect against data loss or breach, including the unauthorized access or use of information that may result in reidentification of pseudonymized data (Recitals 74, 75). Failure to take such steps could expose controllers and processors to potential legal liability (Recital 74). Businesses can also use anonymized data, which must render the data impossible to identify a specific individual. Anonymized data is beyond the scope of the regulation.

Individuals will also enjoy a qualified, affirmative right to erasure and destruction of personal data ("right to be forgotten"), provided that there is no legitimate reason for the information to be retained. Data controllers who have made data public should take "reasonable steps" to inform other controllers and processors that the individual has requested erasure of any copies of, or links to, that personal data. The right to erasure shall not apply to the extent that processing is necessary for complying with a legal obligation under EU or Member State law (including under authority vested in the controller), for processing data in furtherance of a public interest (including public health), for exercising the right of freedom of expression and information, or in furtherance of a legal claim or defense. Under Article 17(3)(d), this right also does not apply for "archiving purposes in the public interest," scientific or historical research purposes, or statistical purposes where "appropriate safeguards" (e.g., pseudonymisation) are employed if it is likely that exercise of the right to erasure would "render impossible or seriously impair" the purpose of processing the data.

Article 8 underscores data controllers' and processors' added responsibilities where children and their data are concerned. Besides singling them out as "vulnerable natural persons" who may not appreciate the risks associated with data processing, children present special challenges when obtaining consent for information society services, such as e-commerce, that are offered directly to them (Recital 75). Children of at least sixteen years of age may provide valid consent for the processing of personal data (Article 8(1)). The processing of personal data of a child below the age of sixteen is lawful only to the extent the holder of parental responsibility over the child provides that consent or authorization. Data controllers must make "reasonable efforts" to verify that the holder of parental responsibility is, indeed, providing consent for processing (Article 8(2)). Practitioners should note, however, that Member States are authorized under the GDPR to lower the age of consent provided that it is not lower than thirteen years of age. Importantly, consent from a child can be withdrawn at a later date, whether or not the data subject is still a child at the time she or he communicates the withdrawal (Recital 65).

### European Union | Tips for Practitioners

- Confirm data is collected for a "legitimate purpose" and minimize the amount of data collected.
- Disclose, disclose, disclose—Data controllers should ensure data subjects are aware of all profiling and automated processing and decision-making.
- Provide consumers with a clear and separate notice about their right to object to data processing and profiling for direct marketing.
- Provide consumers with simple-language explanations about any automated decision-making or profiling, including "meaningful information about the logic involved," so individuals can make informed decisions.
- Check Member State law for further requirements.

### Philippines

The major law pertaining to big data privacy is the Data Privacy Act, Republic Act No. 10173 of 2012. It grants individuals the right to be informed, to object to uses of their personal information, the right to access and correct information, and the right to erase or opt-out of data usage. Personal information, as defined in Section 3(g), refers to "any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."

Sensitive personal information refers to personal information (1) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations, (2) about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings, (3) issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns, or (4) specifically established by an executive order or an act of Congress to be kept classified.

The processing of personal information that is not considered as sensitive or privileged is permitted if not otherwise prohibited by law and when at least one of the following conditions exists: (1) "freely given, specific, informed" consent by the individual, (2) where necessary for the fulfillment of the contract with the individual, (3) where necessary for

compliance with a legal obligation to which the data controller is subject, (4) where necessary to protect "vitally important interests" of the individual, including life and health, (5) national emergency, public safety, or functions of a public authority central to its mandate, or (6) the legitimate interests of the data controller or third party, except where the individual's rights and freedoms are protected by the Constitution.

In case of Sensitive Personal Information, the processing is allowed only if the individual has granted consent for that specific purpose or if it is falls within one of the five exemptions: (1) where provided for by existing laws and regulations, (2) where necessary to protect the life and health of the individual or another individual and the person is unable to express consent prior to processing, (3) where necessary to achieve lawful and noncommercial objectives of public organizations and their associations, subject to additional conditions, (4) for the purposes of medical treatment, subject to adequate privacy and security safeguards, and (5) where necessary for court proceedings, for legal claims, and by government authorities.

## Extraterritorial Application and Cloud Providers

The Data Privacy Act applies outside of the Philippines when it involves personal information about a Philippine citizen or resident or when the entity has a link with the Philippines. The link can include, but is not limited to, a contract entered into in the Philippines; a juridical entity unincorporated in the Philippines but that has central management and control in the country; and an entity that has a branch, agency, office, or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information. It also can include an entity that carries on business in the Philippines. Lastly, it can apply if the personal information was collected or held by an entity in the Philippines.

## Big Data Security Measures

The Implementing Rules and Regulations require a security system to ensure information privacy. The Data Privacy Act provisions regarding security measures, on the whole, require reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data. Businesses must designate a Data Protection Officer, who shall ensure compliance with the laws on protection of data privacy and security. Clear data protection policies must take into account the nature, scope, context, and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects. Businesses also must adopt procedures to address the collection and limits of data collection, access management, system monitoring, and data retention, among others.

Physical security needs to address data access; duties and schedules of personnel involved in data processing; policies and procedures related to the transfer, removal, disposal, and reuse of personal data; and policies and procedures safeguarding against mechanical destruction of files and equipment.

Technical security policies and practices should be implemented and regularly updated, including safeguards against accidental, unlawful, or unauthorized usage; maintenance of confidentiality, integrity, availability, and resilience of processing systems; regular monitoring for breaches; ability to restore availability and access to personal data; regular testing for effectiveness of security measures; and data encryption.

## Big Data in FinTech

FinTech refers to organizations combining innovative business models and technology to enable, enhance, and disrupt financial services. FinTech companies leverage technology and data to provide financial services quickly and conveniently. Big data is changing the financial industry in numerous ways by predictive analytics. A financial company is required to obtain the customer's consent prior to processing the customer information and specifically inform the borrowers that the financial company will submit their credit information to the Credit Information Corporation and maintain the copies of the submitted credit information.

## Philippines | Tips for Practitioners

- Financial companies should include a statement within their Privacy Policy, such as: "That the user agrees that his or her personal information disclosed in this mobile application, necessary for determining the credit score for availing a loan, shall be used by and communicated to [financial company's name], in accordance with the Data Privacy Act of 2012."
- Financial companies should include a statement in the loan/credit applications signed by the borrower, such as: "I hereby acknowledge and authorize: 1) the regular submission and disclosure of my basic credit data (as defined under Republic Act No. 9510 and its Implementing Rules and Regulations) to the Credit Information Corporation (CIC) as well as any updates or corrections thereof; and (2) the sharing of my basic credit data with other lenders authorized by the CIC, and credit reporting agencies duly accredited by the CIC."

## Mexico

The Mexican data protection framework is comprised of: (a) the Mexican Federal Law on Protection of Personal Data Held

by Private Parties (Mexican DPL) issued on July 5, 2010; (b) the regulation of the Mexican DPL; (c) guidelines on privacy notice; (d) recommendations on a personal data security management system by the National Institute for Transparency, Access to Information and Data Protection, which is the federal data protection authority (DPA); (e) parameters for corporate or self-binding rules; and (f) guidelines for data protection, investigation and verification procedures, and imposition of penalties.

The Mexican DPL applies to any person, including an individual or company in the private sector, who processes personal data, and has a presence in Mexico or who processes personal databases out of Mexico. The data controller must provide the individual, as the data subject, with all the relevant information regarding the processing of his or her personal data, through a privacy notice. Processing of personal data will be done as necessary, appropriate, and relevant, according to the purposes set out in the privacy notice. The data subject has the right to access, rectify, cancel, and oppose to the use of his or her personal information.

All processing of personal data is subject to express or implied consent of the data subject. There are certain instances in which neither implied nor express consent is necessary for the processing of personal data. For example, consent is not required when the personal data is subject to a prior deidentification procedure. Processing of personal data must be limited to the purposes set out in the privacy notice. If the data controller intends to process data for a purpose that is not compatible to the purposes set out in the privacy notice, the data subject's consent must be obtained again. The Mexican DPL does not provide specific rules on big data; however, the Mexican DPL is applicable to all types of personal data processing.

## Sensitive Personal Data

Sensitive personal data refers to data that affects the most intimate personal realm of the data subject that may result in discrimination or that creates a potential risk for the same. Examples of sensitive data include, but are not limited to, data regarding racial or ethnic origin; present or future health conditions; genetic information; religious, philosophic, or moral beliefs; union affiliation; political opinions; and sexual preference. When processing sensitive personal data, consent must be expressly granted, and the processing period must be as limited as possible.

## Security Measures and Retention Period

All responsible parties that process personal data must establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction, or unauthorized use, access, or processing. Data controllers cannot adopt security measures inferior to those used in the managing of their own information. Moreover, the risks involved, potential consequences for the data subjects, sensitivity of the data, and technological developments need to be taken into account.

Security breaches occurring at any stage of processing that materially affect the property or moral rights of data subjects will be reported immediately by the data controller to the data subject and the DPA.

Personal data must be retained and stored during its processing by the data controller. When personal data is no longer required it shall be canceled and subsequently deleted. The time of retention of the information will depend on the purpose for which the personal data was collected, legal statues of limitations, and even internal privacy policies of the data controller.

Any disclosure of personal data between a data controller and a third party is considered as a "transfer," whether domestically or internationally, and requires the consent of the data subject, except when transferred within a corporate group ruled under common privacy policies.

## Mexico | Tips for Practitioners

- From the year of the first sanction in 2012 through June 30, 2017, the Mexican DPA has imposed fines of an approximate aggregated amount of USD$18,065,155.
- The most frequently committed violations for which the DPA has imposed fines are: (i) processing personal data without respecting the principles set forth in the Mexican DPL (lawfulness, responsibility, loyalty and consent); (ii) collecting or transferring personal data without the express consent of the data subject; and (iii) omitting certain or all of the provisions required for the privacy notice.
- The sectors in which the DPA has carried out verification procedures more frequently, are: (i) financial and insurance, (ii) scientific and technical, (iii) information in mass media, (iv) business support services, (v) healthcare and social care, and (vi) retail and educational services.

## Brazil

Brazil does not have a unified data privacy law. Data protection is governed by the Federal Constitution, the Defense Code, the Civil Code, and industry specific laws, such as, inter alia, the Civil Rights Framework for the Internet ("Marco Civil da Internet") (Federal Law 12.965/2014) and the Credit Reports Law ("Lei do Cadastro Positivo") (Federal Law 12.414/2011). Brazil is still far from the comprehensive approach to legally

ensured privacy safeguards established in the European Union, Canada, Argentina, and Uruguay, among others.

Basically "consent" is mandatory whenever personal data is processed. Processing data encompasses, "the set of actions related to information collection, production, receipt, qualification, use, access, reproduction, issue, distribution, transport, processing, filing, storage, exclusion, assessment or control of the information, change, communication, transfer, spread or extraction," under Article 14(I) of the Decree that regulates Marco Civil. However, Marco Civil is a limited sectorial law that applies only to internet services.

The Marco Civil calls for freely given, express, and informed consent from the individual at the moment the data is collected. From an international perspective, it is important to be aware that Article 11 of the Marco Civil states the applicability of Brazilian law to companies headquartered outside Brazil, "provided that they offer services to the Brazilian public or at least one member of the same economic group is established in Brazil." This statement applies to "the data collected in the national territory and to the content of the communications in which at least one of the terminals is placed in Brazil" (Article 11(1)).

Compliance with data privacy laws is regulated. Internet Services Providers and Internet Application Providers must provide, as set forth by regulation, "information that allows verification concerning its compliance with Brazilian legislation regarding the collection, storage, retention and treating of data, as well as, in regard to the respect of privacy and of confidentiality of communications," under Article 11(3).

An "opt-out" structure is not compatible with Brazilian law. Decree 05/2002 by the Ministry of Justice states that it is unfair in a consumer contract to create the imposition to "opt-out" if the consumer does not want to have his or her personal information transferred. Under the Civil Rights Framework for the Internet, an internet user's "express consent" is required before collecting personal data (Article 7(IX)), and "free, express and informed consent" is required before personal data transfers under Article 7(VII).

Where violations of privacy and protection of personal data laws provided by Marco Civil occur, no matter if the violations are extraterritorial or do not involve a Brazilian subject's personal data, the following sanctions authorized in Article 12 may be applied individually or cumulatively:

I. a warning, which shall establish a deadline for the adoption of corrective measures;
II. fine of up to 10% (ten percent) of the gross income of the economic group in Brazil in the last fiscal year, taxes excluded, considering the economic condition of the infractor, the principle of proportionality between the gravity of the breach, and the size of the penalty;
III. the temporary suspension of the activities that entail the events set forth in Article 11; or
IV. prohibition to execute the activities that entail the activities set forth in Article 11.

In the case of a foreign company, the subsidiary, branch, office, or establishment located in Brazil can be held jointly liable for the payment of the fine.

In 2016, Decree 8.771/2016 created new general cybersecurity requirements that must be followed by any company that handles personal data. Article 13 requires: (i). the setting of a strict control on data access, including the duties of people who may access it, (ii.) the use of two-factor authentication systems, or other mechanism to ensure the individuality of the responsible for processing the log, (iii.) the need of a detailed inventory on the accesses to connection logs and logs of access to applications, including time, duration, identity of the person responsible for the access, and the accessed file, and (iv.) the use of cryptography technologies or similar protection measures to ensure data integrity. In theory, these requirements are applicable to all digital companies, such as Internet Service Providers and Internet Application Providers, but we have not seen any sanctions for noncompliance yet.

There are five draft bills on data protection being considered in the Brazilian Congress, with a possibility that at least one of them will be approved by the end of 2018. The legislation most likely to be passed is based on both European and Canadian law. Once approved, it will probably take 180 days before the law enters into effect. This future law has the potential to strengthen Brazil's maturity regarding data protection through a broader treatment of personal data, encompassing provisions such as the need of a Data Protection Officer, different consent criteria for sensitive data, processing based on legitimate interests, data portability rights, privacy by design and by default, and the creation of a Data Protection Authority, among others.

In lieu of comprehensive data privacy legislation, lawyers can look to the courts for guidance on what is required for data privacy and the evolving landscape of privacy in the digital age. For example, in 2015, the Superior Court of Justice decided that the use of personal data to calculate credit default risks by using scoring methods is legal as long as the consumer consents to the processing of the data. *See* Superior Court of Justice, Special Appeal 1.304.736/RS, *decided* Feb. 24, 2016. This judgment set some parameters that now govern rules on algorithm accountability. The Supreme Federal Court is also currently deciding cases on the limits of the use

*continued on page 21*

# French Data Protection Rules

By Danhoé Reddy-Girard

## Sources and Scope of Application

French data protection rules are mainly set out in law No. 78-17 of 6 January 1978, as amended in 2004 to transpose European Directive 95/46/EC of 24 October 1995 (the Data Protection Law), and in regulation (*décret*) No. 2005-1309 of 20 October 2005, and are supervised by the Commission nationale de l'informatique et des libertés (the CNIL).

The Data Protection Law applies to the "processing" of "personal data," which is data on individuals allowing them to be identified, by a "controller" established in France or by a controller established outside the European Union but using processing means (other than equipment used only for transit purposes) located on French territory.

The main rules of the Data Protection Law will be replaced by the European General Data Protection Regulation 2016/679 of 27 April 2016 (the GDPR) when the latter enters into force on 25 May 2018. The GDPR has been introduced mainly to ensure a more consistent level of protection for natural persons throughout the European Union and to prevent divergences hampering the free movement of personal data within the internal market, thus providing more legal certainty and transparency for economic operators. The GDPR also aims to provide greater protection to individuals especially with regard to online activity of websites located abroad. The new rules will be overall similar albeit more stringent in certain ways. They will also have a wider territorial scope of application, applying not only to controllers established in the European Union but also to processors established in the European Union and, in case goods or services are offered to data subjects in the European Union or when their behavior is being monitored, controllers and processors not established in the European Union.

## Summary of the Main Rules

When it applies, the Data Protection Law requires that

- any processing follow certain basic "principles" set out in article 6 of the Data Protection Law, namely that personal data be: (a) processed lawfully and fairly; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; (d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; and (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- any processing be "lawful" as per article 7 of the Data Protection Law for amongst others (a) the data subject has given consent to the processing of their personal data, (b) the processing is necessary to comply with a legal obligation to which the controller is subject, (c) the processing is necessary to perform a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract or (d) the processing is necessary for the purposes of the legitimate interests pursued by a controller or a recipient, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject; personal data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, health or sex life not be collected or processed and data on criminal convictions or related security measures not be processed, with some exceptions;
- the controller file with the CNIL a declaration or, in certain cases, an authorisation request. The CNIL has adopted simplified norms for most of the usual processings performed by businesses such as for managing badges ("Norm No. 42"), employees ("Norm No. 46"), calls ("Norm No. 47"), clients and prospects ("Norm No. 48"); these can be declared using a simplified declaration. The CNIL has also exempted certain processings, such as in respect of supplier data and, only when collected outside the European Union by controllers established outside the European Union who fall within the scope of application of the Data Protection Loan only because they use the services of a processor located on French territory, certain employee and client data. A normal (not simplified) declaration is required for most other

**Danhoé Reddy-Girard** is a partner with Gowling WLG in Paris, France.

processings, such as for video monitoring, for providing Wi-Fi access to nonemployees, and for implementing a program to promote equality amongst staff of different ethnic origins or sexual orientations. A normal declaration must contain information about the objective of the processing (one per declaration), the recipients, the maximum storage period and other information as set out in Article 30 of the Data Protection Law. No declaration is required if a personal data protection correspondent is appointed, this appointment is notified with the CNIL and the processing does not entail any transfer of personal data outside the EU. An authorisation is required in certain cases, such as for implementing a whistleblowing programme (which is now required for businesses with at least 50 employees);

- the controller provide data subjects with certain information as per article 32 of the Data Protection Law (such as information on his or her rights as well as on whether the controller intends to transfer personal data to a country outside the EU, whereupon article 91 of regulation (*décret*) No. 2005-1309 requires additional information to be provided: the names of the relevant countries, the information to be provided, the purpose of the transfer, the categories of transferees in such country, the level of protection afforded in said country such as if the country is in the European commission's approved list), and as per the relevant simplified norm as appropriate, if either (a) the data is collected by the controller or (b) the data is collected by someone else if providing this information to data subjects is not impossible and would not involve disproportionate efforts, and this information has not already been provided;
- the controller take appropriate measures to preserve the security and confidentiality of the databased on the type of personal data to be protected. The CNIL has issued specific recommendations in this regard;
- the controller ensure that any processor (meaning any person asked by the controller to process personal data on its behalf) provide sufficient guarantees to preserve the security and confidentiality of the data and enter into the contract with adequate clauses as per article 35 of the Data Protection Law. The GDPR will also saddle processors with obligations;
- data not be stored for longer than is necessary for the purposes for which the personal data are processed (except rare exceptions);
- data subjects can request from the controller access to and rectification of personal data concerning the data subject as well as (in the absence of contrary provision in the relevant contract) object to the processing of such personal data for legitimate purposes. Special provisions apply to children. Furthermore, Norm No. 48 provides that customers may object to (and must be informed that they can object to) the use for prospection of their personal data and transfer thereto to commercial partners for prospection purposes; and
- no personal data be transferred to a country outside the EU that is not offering an adequate level of protection except where the processing itself offers that level of protection, for instance by the use of the EU standard clauses or binding corporate rules or reliance on the new U.S. "Privacy Shield" accreditation (replacing the U.S. Safe Harbor accreditation).

## Special Rules on Cookies

Rules pertaining to cookies were introduced in article 32 II. of the Data Protection Law for the purposes of transposing European directive 2009/136/EC of 25 November 2009.

Article 32 II. saddles the "controller or its representative" with the obligations to inform (and obtain the consent) on the use of cookies and similar devices. However, controllers established outside France (including those established in another EU country) are better off making sure their cookie policy complies with French rules, even if only in order to trade with French advertisers, as the CNIL considers advertising agencies, social networks and analytics firms as controllers.

To be compliant with French law, for all cookies other than strictly necessary cookies (including functionality cookies and performance cookies, assuming the latter would not meet a 6-prong test to be exempt from the consent requirement), a positive consent is required.

According to the CNIL, a proper way to obtain that consent is to use a banner that reads: "By continuing browsing on this site, you accept the use of [Cookies or other trackers] for offering you [For instance, targeted advertising publicity aiming your centers of interest] and [For instance, computing visit statistics]. In order to know more and for parameting the trackers," with this last sentence containing a hyperlink to the policy and possibly tick boxes to deactivate cookies according to their finality category. The banner should remain on the page until the user clicks on a button in the page; it must not fade out if the user does not click on a button.

In France, the CNIL considers that the consent should be valid for thirteen months as from the installation of the cookie (CNIL, délib. n° 2013-378, 5 déc. 2013) so cookies should expire after thirteen months.

## Special Rules on Direct Marketing

Direct marketing "using the details of individuals" through automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail is regulated by article L.34-5 of the Code des postes et des communications, transposing European directive 2002/58/EC (Privacy and Electronic Communication) of 12 July 2002.

These provisions apply to controllers who fall within the territorial scope of application of the Data Protection Law. However, controllers established outside France that fall outside the territorial scope of application of the Data Protection Law are advised to comply with these French rules on direct marketing when targeting the French market; a foreign company would not be able to go to French advertisers with its list of potential clients without justifying to them that the opt-in requirement has been satisfied.

Article L.34-5 provides that direct marketing "using the details of individuals" through automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail is prohibited unless either

- the individual has given his or her express ("opt in") consent,
- the individual has already purchased from this very company goods or services "analogous" to those being advertised (and at the time personal data was collected about this individual, this was done in compliance with applicable data protection rules and the individual was given the opportunity to opt out from future advertising using his or her personal details); or
- the unsolicited communication is in respect of a non-profit cause.

Although this is not exactly how Article L.34-5 is written, the CNIL, under pressure from lobby groups, has issued guidelines providing that the above rules (requiring "opt-in") do not apply to emails to individuals acting not as consumers but as professionals, including employees of legal entities, where the solicitation is in relation to the profession of that individual. The CNIL's guidelines provide an example of the IT director of a company, to whom IT services could be offered. In that case, there is no need for the individual to have "opted in" or to have purchased analogous goods or services in the past, but the individual is nevertheless entitled to be informed upon his or her email address being collected that it may be used for solicitation and that he or she has the right to opt out. Solicitation to company email addresses that do not contain the name of an individual (e.g., those starting with "contact@ . . .") are not covered.

In all cases, any message must identify its author and allow the recipient to subsequently opt out.

The maximum period one can keep personal data on individuals who are not clients or employees should also be respected (this time period is typically 3 years for entities that filed a Norm No. 48 simplified declaration to the CNIL).

## Monitoring and Sanctions

The CNIL can carry out an investigation and issue a notice enjoining the violating person to remedy the situation within a certain period, which can be 24 hours in case of extreme emergency. If this notice remains unanswered,

- the violating person can be fined up to €3,000,000; and/or
- an injunction to stop the violating processing may be ordered against the violating person (and withdrawal of the authorisation in case of a processing subject to authorisation).

Blocking access to CNIL agents carrying out an investigation, refusing to communicate information to CNIL agents and communicating false information to CNIL agents are offences that can be sentenced with one year of jail and a fine of €15,000.

Notwithstanding the sanctioning powers of the CNIL, most breaches of the Data Protection Law are offences that can be tried in court with a maximum jail sentence of 5 years and a maximum fine of €300,000 (or five times this amount for a legal entity). Failure to communicate to data subjects the information required by article 32 of the Data Protection Law is however only a 5th category minor offence (contravention) for which there is no jail sentence, and the maximum fine is €1,500 or €3,500 in case of a repeated offence (or five times this amount for a legal entity). In practice, the CNIL is unlikely to ask the general attorney to commence criminal proceedings without first having tried to address the non-compliance, assuming it is not an outrageous violation.

Breach of article L.34-5 of the Code des postes et des communications is sanctioned by a fine of EUR 750 fine for an individual, or EUR 3750 for a company, per communication. It can also lead to a maximum €15,000 administrative fine imposed by the authority in charge of protection of competition and consumers, unless article L.36-11 of same code applies and the authority in charge of electronic communications takes jurisdiction.

In summary, French data protection rules do not merely require one to make a declaration to the CNIL but sets out other rules, like storage limitations and information obligations, and extend to consent to cookies and to direct marketing.

In addition to the GDPR's expanded territorial application, some of the key changes that it will bring when it enters into

force are requirements for controllers and processors to establish written procedures and for additional information to be communicated to data subjects. It also replaces the current declaration/authorisation obligation with obligations to conduct a data protection impact assessment where the contemplated processing "is likely to result in a high risk to the rights and freedoms of natural persons" and to consult the CNIL if such assessment indicates that the processing would "result in a high risk in the absence of measures taken by the controller to mitigate the risk."

A European Union "Regulation on Privacy and Electronic Communications" is also being currently prepared. The leaked draft suggests it would become effective at the same time as the GDPR and will modify the above rules on cookies and on direct marketing. ◆

# Cybersecurity Checklist when Using Outside Vendors

## From the ABA Cybersecurity Legal Task Force

The ABA Cybersecurity Legal Task Force has developed a range of guidance to help law firms, attorneys, and their clients effectively manage cybersecurity risks. Its "Vendor Contracting Project: Cybersecurity Checklist" focuses on one aspect of cybersecurity risk, namely vendor relationships, including best practices when selecting and working with supply-chain vendors or partners. The checklist provides guidance on cyber risk-management assessment, vendor security practices, and contract considerations to set expectations, mitigate risks, and allocate liability.

The following excerpt from the Cybersecurity Checklist offers basic principles, lessons, and strategies for addressing cybersecurity threats and third-party risks. It contains valuable tips on the essentials for understanding information security activities, assessing cyber risks, and conducting due diligence. Legal practitioners can find additional in-depth discussion and guidance on contractual provisions in the full toolkit online. An appendix provides sample contract provisions covering data protection of personally identifiable information, using Canadian law as the example. The Cybersecurity Checklist and ongoing updates can be found on the ABA Cybersecurity Legal Task Force website, https://www.americanbar.org/groups/public_services/law_national_security/cybersecurity.html.

### Overview

The objective of the Cybersecurity Checklist is to assist procuring organizations, vendors, and their respective counsel to address information security requirements in their transactions. The Checklist frames the issues parties should consider consistent with common principles for managing cybersecurity risk. The Checklist contemplates transactions from due diligence and vendor selection through contracting and vendor management. It suggests that cybersecurity provisions are not "one-size-fits-all," but should instead be informed by parties' assessment of risk and strategies to mitigate risk.

For convenience, the Checklist uses the term "vendor" to refer broadly to any third-party supplier of goods or services and the term "purchaser" to refer broadly to the party receiving the goods or services. The term "agreement" is used in the Checklist to refer to a product purchase agreement, license agreement, service agreement, or other agreement however styled to reflect the nature of the arrangement between the vendor and purchaser.

The ABA Cybersecurity Legal Task Force recognizes that cybersecurity is a dynamic subject. Practitioners are encouraged to modify and supplement the Checklist to reflect the particular regulatory requirements and business needs of their clients. Additional guidance can be expected over time.

Further, there are many sources of law and guidance that may inform an organization's cybersecurity strategy and measures to protect and secure data in electronic form containing personal information. Most U.S. states, and some Canadian provinces, have breach notification laws triggered by loss of personally identifiable information or other sensitive information. Organizations with global business operations must comply with applicable country-specific laws and may be subject to rules of intergovernmental organizations, e.g., European Union, Canada, the Association of Southeast Asian Nations, Asia-Pacific Economic Cooperation, and others.

The Cybersecurity Checklist was prepared by ABA members Cheryl M. Burtzel (Austin, Texas), Candace M. Jones (New York, New York), Lisa R. Lifshitz (Toronto, Ontario, Canada), and Lucy L. Thomson (Washington, D.C.) with valuable feedback from other members of the ABA Cybersecurity Legal Task Force, the Business Law Section, and the Section of Science and Technology Law.

### Cybersecurity Strategy: Understanding the Landscape of the Transaction

An organization's information security activities should begin before it undertakes transactions as vendor or purchaser. All organizations should establish and maintain a documented strategy for identifying and managing their respective cybersecurity risks. An organization's cybersecurity strategy should be informed by laws and regulations—federal, state, local, and international (at national, regional, provincial, and local levels)—to which the organization is subject, applicable industry standards, and business and operational requirements, including the organization's assessment of its own tolerance for risk. In some cases, applicable law may mandate specific terms for

vendor agreements, such as Business Associate Agreements required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), U.S. government contract provisions in supplier agreements, and Privacy Shield Principles mandated for organizations handling personal data of individuals in the EU (even if the contracting parties are outside the EU). Transactions that introduce third parties into an organization's business operations, whether as vendor or customer, should be accounted for in the organization's business and risk strategies. Conversely, transaction terms should account for the organization's cybersecurity strategy.

From the purchaser's perspective, vendor selection should also be informed by the purchaser's specific requirements and expectations regarding the information and information systems relevant to the vendor relationship. These requirements should anticipate controls the purchaser will implement and maintain as part of its overall information security plan for the business activity. The purchaser should have an informed and realistic view of its own environment and business needs so that it can reasonably assess the impacts (small or significant) of introducing a vendor relationship and make appropriate business judgments consistent with the purchaser's risk tolerance as well as applicable regulatory and legal requirements. Depending on the nature of the goods or service and the interconnectedness of the vendor and the purchaser, new vendors may introduce or increase information security risk, mitigate security risk, or both. Among other things, the purchaser should clearly understand the service delivery model and approach proposed by the vendor, including the vendor's proposed use of subcontractors and suppliers who may have access to or impact the purchaser's systems and data. The purchaser should also plan adequate resources to implement and maintain appropriate vendor management practices.

From the vendor's perspective, the vendor must understand how a purchaser's requirements could affect the vendor's operations. For example, supplying products or services to a purchaser in a regulated industry such as financial services or healthcare may impose requirements not addressed in the vendor's current procedures, systems, or compliance processes.

In most organizations, understanding the landscape into which a new vendor/purchaser will be introduced or new product or service will be added is a cross-functional exercise involving the people in the organization who understand the business objectives, the business process—particularly the participants and information involved—the information systems, and the organization's risk tolerance and risk-management practices. While transaction planning will be driven by individuals responsible for the business activities to be supported by the product or service to be purchased/supplied, transaction planning should also leverage individuals tasked by the organization with responsibility for implementing, managing, and overseeing the effectiveness of its cybersecurity strategy. Organizations with established written cybersecurity governance frameworks should be better equipped to plan for and implement new or changed vendor-purchaser relationships in the ordinary course of business.

## Risk Assessment: Cybersecurity Considerations for the Transaction

Organizational risk comprises many types of risk, e.g., management, investment, financial, legal, safety, logistics, supply chain, and security risk. Similarly, security risk has multiple dimensions. The Checklist focuses on one aspect of cybersecurity risk, namely vendor relationships. Analyzing interconnections with and dependencies on third parties is an element of cybersecurity risk assessment and management. Ultimately, organizations need to manage risks across the various dimensions enterprise risk strategies should consider how activities to assess and manage risks should inform and influence plans for managing third-party cybersecurity risk and how plans for managing vendors roll up into the comprehensive view of enterprise risk. Adapting the Checklist for any particular organization should account for the organization's enterprise risk strategies and infrastructure.

In general, risk assessments should identify functions, activities, products, and services and their relative importance to the organization. Risk assessments can inform decision-makers and support the risk-management process by identifying:

1. relevant threats to the organization or threats directed through third-party entities
2. vulnerabilities both internal and external to the organization
3. the impact (i.e., harm) to the organization and individuals that may occur given the potential for threats exploiting vulnerabilities; and
4. likelihood that harm will occur.

Organizations should also evaluate the inherent cybersecurity risk presented by the people, processes, technology, and data that support the identified function, activity, product, or service and assess the existence and effectiveness of controls to protect against the identified risk. Thus, risk assessments can provide the basis for the selection of appropriate controls and the development of remediation plans so that risks and vulnerabilities are reduced to a reasonable and appropriate level.

In the vendor context, risk assessments should inform the underlying decision to outsource any function or activity,

as well as the specific requirements for a product to be supplied or service to be performed. Risk assessments and controls should also be referenced in the vendor due diligence and selection process to identify gaps or deficiencies that will need to be addressed by the parties to mitigate risk. At the end of the day, it is in the interest of both vendor and purchaser to identify and mitigate cybersecurity risk.

The parties' cybersecurity strategies and risk assessments will be key to establishing a solid foundation for the vendor selection process. At the vendor selection stage, the prospective purchaser should consider the following:

1. The nature of the goods or services to be purchased/supplied and identify the information and assets relevant to the vendor engagement. What information will the vendor receive from the purchaser, collect on the purchaser's behalf, process, transmit to third parties, and/or store? How sensitive are the data? Do the data include personally identifiable information ("PII"), financial information, protected health information, proprietary information and trade secrets? The inventory of relevant data should include data stored on networks, in third-party data centers, on mobile devices (laptops, portable storage, smartphones), in the cloud, on back-up devices, and in industrial control systems.
2. What is the purchaser's risk profile for the product or service needed? That is, what: (a) information will be processed or stored; (b) access to systems or internal operations will be given to a vendor; and (c) customer-facing activities will be impacted? Does the product or service support critical operations? Will the vendor interact directly with the purchaser's customers or clients or have access to systems or portals through which customers or clients interact with the purchaser?
3. What access will the vendor or purchaser need to have to the other party's information or information systems? What controls does the party whose systems will be accessed have in place to manage such third-party access to its information or information systems? A re the existing controls likely to be appropriate for managing the party to be given access?
4. What are the applicable legal/regulatory requirements for the product or service in the context of the purchaser's business? Does the vendor have experience supplying the relevant product or service to others in the purchaser's industry? Legal requirements from multiple jurisdictions (federal, state, local, and international) and regulatory disciplines (e.g., financial, healthcare, consumer) may apply.
5. What are the applicable commercial requirements, including obligations to the purchaser's customers or business partners, to protect information the purchaser processes or stores for those third parties?
6. What interdependencies will be relevant to effective management of the vendor? Purchasers need to consider the web of customers, vendors, and affiliates who may have a role in delivering or using the product or service or whose information may be provided to the vendor.
7. Will the vendor be providing the goods and services exclusively or will it be working with third parties, including subcontractors? Purchasers will require a good understanding of the prospective vendor's subcontractors and downstream partners as the use of multiple subcontractors and third-party providers will further impact and complicate vendor due diligence and cybersecurity management.
8. What power or influence do the parties exercise in the relevant marketplace? If the negotiating power of either party is outsized relative to the other, responsibility and risk may not be allocated in a way that aligns rationally with the role each party will have in the transaction or the ongoing supply of the product or service. In any case, a party that does not get what it believes is necessary to address its information security expectations will have to determine how, if at all, it can implement controls that mitigate the deficiencies it perceives in the relationship (compensating controls) or it may have to consider other options, including other vendors or other ways of satisfying the business need or otherwise mitigating risk as well as the possibility of covering some risk through the purchase of cyber liability insurance, for example.

## Vendor Due Diligence

As part of the vendor selection process, purchasers should evaluate the capacity of prospective vendors to follow appropriate information security practices in producing and delivering goods and performing services. The purchaser's assessment of its own business and risk-management objectives should inform the purchaser's due diligence activities. See Appendix B of the online text for additional information.

Vendors also learn through the due diligence process about the prospective customer's cybersecurity requirements and expectations. In many cases, vendors have more experience and a deeper understanding of relevant systems and cybersecurity threat landscape than their customers. Vendors may seek through their own due diligence information about the purchaser and

third p arties with which the purchaser expects the vendor to interact. Cybersecurity is not a zero-sum proposition; both parties have an interest in identifying appropriate controls and placing responsibility where risk can best be mitigated.

The parties should be assisted by qualified information security personnel during due diligence and throughout the vendor relationship, as appropriate. To the extent weaknesses are identified during the due diligence phase, the parties' business people (informed by their information security experts) will need to weigh the risks of those deficiencies against the benefits of the transaction and consider appropriate mitigation. This initial assessment and the plan for any agreed remediation should inform the agreement. After completing its due diligence, the purchaser may also need to reassess its risk profile to account for risk arising from the vendor relationship that the purchaser will need to manage. The parties also will need to asses s risk as their respective environments change or whenever additional products or services are implemented.

Due diligence activities generally should accomplish the following:

1. Conduct a security assessment of the vendor, which may be a direct assessment by the purchaser or its agent, review of vendor self-assessment or third-party assessment reports, or some combination of those activities. The scope of the security assessment should be informed by the nature of the product or service, its relative importance to the purchaser, and the sensitivity of information the vendor will collect, store, process, or transmit for the purchaser. Qualified information security personnel should assist the purchaser to identify relevant areas of assessment and to evaluate the information provided by prospective vendors. A complete security assessment guide is outside the scope of the Checklist. Parties should consult employees and advisors with appropriate security expertise. At a high-level, a security assessment generally should consider the extent to which the vendor:
   a. has adopted opposite security policies and procedures, including written policies as necessary to create a "culture of security," and enforces its security procedures, particularly those most likely to prevent the most common types of data breaches;
   b. has created appropriate incident response and business continuity/ disaster recovery (BC/DR) plans and tests and updates them regularly;
   c. maintains a program to manage compliance with applicable federal, state, local, and international laws, including laws prohibiting unfair or deceptive practices, data breach, data disposal, privacy and confidentiality of personal information and other protected records, as well as laws or regulations that restrict use of certain information without appropriate consent; and
   d. addresses information security in a manner that enables the purchaser to demonstrate the purchaser's compliance with applicable laws and regulations, taking into account controls the purchaser inherits from the vendor.
2. Assess the vendor's program to maintain its IT infrastructure and operations consistent with cybersecurity objectives, including those of the purchaser. To what extent does the vendor implement and use software and hardware with security and privacy built into the design of the product? To what extent does the vendor assess the secure development practices of third parties supplying custom and critical applications? How does the vendor monitor its systems for known vulnerabilities and respond to newly - reported vulnerabilities? Does the vendor have a procedure to monitor vulnerabilities identified in authoritative sources and other threat intelligence? Does the organization adhere to practices of scanning software for vulnerabilities before it is installed and for avoiding implementation and use of software and hardware for purposes for which they were not designed? Where and when does the vendor encrypt data in its possession or control? Does it send any data over unencrypted channels?
3. What incidents/breaches and vulnerabilities has the vendor identified in the vendor's systems (including systems provided to it or hosted by the vendor's suppliers and service providers) and what are its plans for remediation? The information requested from the vendor should be reasonable under the circumstances and tailored to the type of product or service the vendor will provide. For example, the parties should anticipate closer scrutiny when the vendor will have access to sensitive customer data or PII, provide a product that affects the security of an organization broadly, or will be a key part of the purchaser's critical infrastructure. If a vendor is not willing to provide the requested in formation, consider what assurance s the purchaser should request about how the vendor manages vulnerabilities and incidents, generally? In this context, the parties may also have an interest in knowing about their counterparties' experience in matters involving law enforcement or regulatory authorities as well as communication plans and infrastructure in place to communicate if/when an incident occurs.

### Contract Provisions: Setting Expectations, Mitigating Risk, and Allocating Liability

The material covered in this list is intended to highlight provisions that should reflect information security considerations even though the substance of the provisions is not necessarily limited to information security. The Checklist does not cover contract terms not likely to reflect information security considerations (e.g., payment terms). The agreement between the purchaser and selected vendor should contemplate the entire vendor lifecycle, including performance monitoring, effective communication (including information about cyber threats and incidents), performance obligations of the parties, and winding up and off-boarding activities at the end of the relationship (including the secure return/erasure of the purchaser's data).

Contract provisions, including elements that address cybersecurity, are not one-size-fits-all. As reflected in the commentary above about cybersecurity strategy and risk assessment, contract provisions should be appropriate for the transaction and, of course, reflect the mutual understanding of the parties. Because all parties to a transaction have a shared interest in identifying and mitigating cybersecurity risk, many provisions relevant to cybersecurity necessarily define processes and allocate responsibility.

The full content of the Cybersecurity Checklist, including sample contract provisions, and ongoing updates can be found on the ABA Cybersecurity Legal Task Force website, https://www.americanbar.org/groups/public_services/law_national_security/cybersecurity.html. ◆

# Take Precautions to Protect Your Clients when Bringing Devices across Borders, Experts Say

By ABA Media Relations

ABA members have been voicing concerns about searches of lawyers' devices at the U.S. border "and the risks that those searches posed to the privileged and confidential information which is maintained on those electronic devices," said retired U.S. District Court Judge in Southern Court of New York Shira A. Scheindlin, now of counsel with Stroock & Stroock & Levan.

In response to those concerns, then ABA President Linda Klein sent a letter to the Department of Homeland Security asking them to revise the current directives, and in late June she and members of the ABA's Governmental Affairs Office met with representatives of the U.S. Department of Homeland Security to discuss these concerns. These efforts will continue, she said.

Scheindlin moderated the program "Prying Eyes: Think Confidential and Privileged Client Information is Safe at the Border? Guess Again," held at the ABA Annual Meeting in New York City and sponsored by the ABA Center for Professional Responsibility.

She shared U.S. Customs and Border Patrol (CBP) statistics, which show that electric device searches are on the rise:

- FY 2015: 8,503 travelers' devices were searched.
- FY 2016: 19,033 travelers' devices were searched.
- First 6 months of FY 2017: 14,993 travelers' devices were searched.

The CBP website lists reasons someone may be chosen for an inspection of electronic devices:

- Your travel documents are incomplete or you do not have the proper documents or visa.
- You have previously violated one of the laws CBP enforces.
- You have a name that matches a person of interest in one of the government's enforcement databases.
- You have been selected for a random search.

CBP does not need probable cause to do a search now, Scheindlin said, but a proposed bi-partisan Border Privacy Bill in the Senate would require CBP to show some probable cause.

According to CBP, "no court has concluded that the border search of electronic devices requires a warrant, and CBP's use of this authority has been repeatedly upheld. This includes a review by the Fourth and Ninth Circuits Courts of Appeals, which approved the search of electronic devices encountered at the border."

Furthermore, "Electronic device searched are integral in some cases to determining an individual's intentions upon entering the United States," said Deputy Executive Assistant Commissioner, Office of Field Operations, John Wagner. "These searches, which affect fewer than one-hundredth of 1 percent of international travelers, have contributed to national security investigations, arrests for child pornography and evidence of human trafficking. CBP officers are well trained to judiciously conduct electronic device searches and to protect sensitive information that may be encountered."

Scheindlin said the "border" is officially defined as a 100-mile zone around the actual border and that, while border agents can deny entry to a foreign visitor, they cannot deny entry to a U.S. citizen.

Refusing access to a device can result in it being confiscated or its contents being copied, she said.

The panel reviewed the law and what CPB can and cannot search for.

Maureen T. Kelly, assistant general counsel at Northrup Grumman, said the Fourth Amendment is designed to protect us against unreasonable search and seizure, and a key cornerstone of it is the "reasonableness" issue.

Bruce A. Green, director of Louis Stein Center for Law and Ethics at Fordham Law School, said the Supreme Court has said you can be searched at the border, where they are looking to see if you have plants or some other item you are not supposed to bring in to the United States, such as child pornography or anything terrorism related.

But the device(s) you're likely carrying are storing a lot of information that you want to keep private.

Prior to the Supreme Court's decision in *Riley vs.*

*California*, Green said, there was a Ninth Circuit en banc decision that said if border agents are doing not just a cursory look but a "deep dive" into everything on a device, they need to have reasonable suspicion.

Then in the 2014 *Riley* case, he said, the Court unanimously held that the warrantless search and seizure of digital contents of a cell phone during an arrest is unconstitutional.

Kelly said border agents can ask for the password to the device, and you can provide it but that you should say that you do not consent to the search.

There is a lot here tha is murky and yet to be decided, she acknowledged. It is clear they can take a cursory review of your device, but where is the line where it becomes invasive?

Steven M Puiszis, a lawyer at Hinshaw & Culbertson in Chicago, said agents can look at your social media if it is accessible through an app on your phone, but not if it is accessed through an external server or the cloud.

Speaking of a lawyer's ethical obligations, Green said Model Rule 1.1, dealing with competence, says lawyers need to know relevant technology.

Therefore, he said, lawyers have ethical obligations when bringing devices across the border if they contain attorney-client information, including e-mail, documents, etc. A lawyer must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation of a client, he said.

If you lose your device and it has client information on it, Green said you need to inform the client of this, too.

In terms of digital self-defense, Puiszis advised looking at the situation from a risk-management perspective. Ask yourself, "Do I need this information on my phone for this trip?' If not, don't take it, he said. He recommends lawyers traveling to Russia or China use burner phones and laptops because of the higher likelihood of those border agents looking at devices.

Another alternative, he said, is to take your own devices but have the firm e-mail taken off, clear your browser, and take off any social media apps. In addition, move any documents off the hard drive and onto a shared drive.

Even if you are a solo practitioner, Green recommended moving toward these practices and said it is cheaper to do so than you think.

If you are stopped at the border and you have client information on your device, Green said you cannot offer to hand over that information if there are other alternatives available.

He suggested calling your firm's IT department and having the device wiped from afar.

And the panel stressed making sure that you note that you do not consent, resist by asking to see the manager,, and eventually even litigate, if possible.

The panel agreed that you need to know your rights by knowing the laws of the countries where you are traveling. ◆

## Big Data

*continued from page 10*

of encryption (*see* WhatsApp Case, Superior Court of Justice, Direct Action of Unconstitutionality, 5527, *decision pending*; Claim of Non-compliance with a Fundamental Precept 403, *decision pending*) and on the implementation of the so-called "right to be forgotten" (Federal Supreme Court, Extraordinary Appeal 1.010.606, *decision pending*).

### Brazil | Tips for Practitioners

- Companies and organizations should obtain consent from an individual based on an "opt-in" requirement in order to collect or transfer personal data.
- Consent is usually obtained by the user's express acceptance of a clear "Privacy Policy" and/or clear contractual clause. The clauses should be highlighted and separate from other statements. It is not necessary to have "written consent," particularly in the online context.
- There are no data localization requirements in Brazil, except for the financial sector.
- Individuals may request the complete deletion of personal data collected from internet applications. ◆

# Global Legal Market

## Law Firms Go beyond the Merger

By Norman Clark

An attractive, growing legal market inevitably attracts new competitors. Local law firms, which for purposes of this discussion include law firms that are located in only one jurisdiction, inevitably find themselves having to navigate new currents in a maturing legal market with new competitors, many of which are larger, better-resourced outsiders. The firm in New York or London that used to refer work to the firm now has an office across the street and is competing head-to-head for many of the same clients.

Local law firms have responded to the maturation of the global legal market through a variety of structures to improve their international visibility and, more importantly, their service delivery capabilities: de jure and de facto mergers with other law firms; global networks; joint ventures; strategic alliances; and "best friends" relationships. Each structure, in its many variants, offers substantial opportunities to serve clients better, improve financial performance, and maintain competitiveness in a tightening, much more competitive, legal market.

The recent law firm combinations at the national and regional level activity suggest that, barring any major global economic dislocations, the next five to eight years will be a period of increased consolidation of local legal markets, especially in the practice areas and among the client sectors that traditionally have been the provinces of small and midsize local firms. Maybe, as some have suggested, the momentum and mass of "big firm" cross-border combinations will slow as national markets become saturated with large international firms. Maybe not. But one can expect to see much more merger activity among midsize and small firms, especially within a single country, as well as internationally.

**Norman Clark** (*www.walkerclark.com*) is one of the founders of Walker Clark LLC and is co-chair of the Transnational Practice Management Committee.

Does this mean that merger will become the preferred strategic option for small and midsize local law firms that want to maintain their market positions or, in some instances, just survive? A merger is not the only answer, or even necessarily the preferred one. Increasingly, more law firms are considering whether a non-merger option might be a good strategic choice, and, if so, which option will be the best investment for their firms.

### Which Local Law Firms Might Benefit from Change?

With internationalization of the legal market, the number-one challenge to small and midsize local firms in a rapidly changing legal market is profitability. Local law firms need to pay close attention not only to protecting the firm's profitability but also to making it sustainable into the future. Small and midsize law firms should start considering now what strategies will produce the best return on their investment, especially in terms of sustainable financial performance and market position in environments that are likely to be more competitive than ever before. A firm that waits until 2020—or even 2018—might find that the rest of the market has passed it by, and that it will be almost impossible to catch up without profound sacrifices.

At least three categories of local law firms are at potentially higher risk from the impacts of internationalization:

"Leading" national firms in markets that have recently been entered by foreign law firms. In this regard, we believe that national law firms in South Korea, Turkey, and many jurisdictions in Africa are particularly vulnerable. We also see risks for national law firms in the Russian Federation and increasingly in the major markets in Latin America.

Small firms in more mature legal markets, such as the United States, Canada, and the United Kingdom, will find it more difficult to compete unless they radically and innovatively rethink their limited service delivery capabilities and improve how they communicate their competitive advantages to increasingly sophisticated clients.

In markets where the leading law firms are quickly transitioning from "family" firms to "institutional" ones, the "family" firms frequently lack the internal governance and performance management structures that they will need to keep up with their "institutional" local competitors and with foreign firms.

### Is a Merger the Only Answer?

There appears to be a "merge or die" or "grow or die" resignation appearing in many small and midsize local law firms. However, a merger—whether by acquisition or through a de facto merger such as a *Verein* structure—might not be best strategic option for many law firms.

Pay close attention to the recent flurry of merger discussions among midsize law firms. Unlike merger

discussions in local firms during the past five years, many of which have tended to be motivated by a defensive strategy—i.e., increase size to protect the firm's ability to compete—many of the most recent discussions among smaller local law firms appear to be aimed at expanding market share and increasing the client base, rather than just maintaining it, In other words, this is part of a growth strategy, not just a set of improvised responses by which a firm hopes to protect the status quo.

## What Are the Nonmerger Options?

It is not a choice of "merge or die" or "grow or die" for most well-managed local law firms. There are other "nonmerger" structures for affiliation, alliance, or association that are available to law firms that want to extend their geographic presence or service capabilities without going into a full merger, for example:

- law firm networks
- multidisciplinary networks
- specialized practice networks
- highly integrated regional groups of law firms
- bilateral strategic alliances and joint ventures
- combinations with other financially autonomous law firms practicing under a common brand

Some law firms also prefer to build their own networks of one-to-one strategic relationships or alliances through nonexclusive and informal relationships. The same principles that govern a consideration of traditional networks also apply to "do it yourself" and "best friends" networks.

So, if you are part of a small or midsize law firm looking for opportunity, think about your new foreign competitors not just as competitors, who can make you more competitive; but also consider them as potential collaborators, referring to you sophisticated legal work requiring a level of experience and expertise in the local business and regulatory environment that they cannot deliver onsite.

## Is a Network a Good Strategic Choice for My Law Firm?

First, have clear goals before joining a law firm network. Consider network membership as a strategic tactic, rather than a strategy by itself. In other words, how would participation in a network materially support the achievement of a specific strategic goal for your firm? If your firm has not defined strategic objectives that are specific, measurable, realistic, agreed by all the partners, and defined by time limits, then the decision to join a network will be little more than wishful thinking, and the selection of a network will be little more than guesswork.

The direction and extent of the investigation and analysis will vary according to the nature of the proposed affiliation and the strategic position and priorities of the firm. Nonetheless, law firms should invest the time and resources necessary to ensure that they make well-informed, intelligent decisions. Taking intellectual short cuts to quick decisions increases the probability of disappointing results or, worse yet, actual harm to the firm's business performance and strategic position.

### *What Is the Strategic Business Case?*

Adopt a "merger mentality" even when it's not a merger. Although the opportunities and risks presented by these forms can be significantly different, law firms should use substantially the same methodology that they would use for a traditional merger. As with a formal merger, the first question to be considered in any combination or affiliation with another law firm is "Why should we do this?" This involves three basic actions, each of which should be undertaken with clarity and intellectual discipline: identify and quantify the synergies, identify and define the risks, and estimate the probable return on investment.

Questions to consider as part of your assessment include:

1. What are the tangible and intangible investments that the partners must make—especially the investment of their time—to produce the best results for their firm?
2. What external and internal value will each relationship deliver?
3. What makes you different from other law firms?
4. What specifically do you do better than your competitors?
5. What will your law firm bring to the relationship?

### *Conduct Cultural Due Diligence*

Most law firms do an excellent job of conducting due diligence into the financial performance and client base of a prospective partner for a merger or other strategic alliance. Few firms, however, conduct an adequate cultural due diligence. Cultural due diligence is not just whether the partners of the two firms like each other. Instead, it examines a range of issues with respect to decision making, planning, practice management, and group performance to identify potential incompatibilities that, unless adequately managed, would prevent the combination, affiliation, or merger from achieving its full potential. It is probably the most important risk management tool in any combination of two or more firms and is particularly important for cooperating with other firms across countries, legal systems, and cultural and societal practices.

## How Can My Law Firm Leverage Networks for Growth?

Network membership should be linked to significant, articulated, and measurable strategic objectives. Law firm partners should be able to anticipate, with reasonable specificity—even if not with clairvoyance—the nature, quantity, quality, and value of the opportunities that a network will provide.

***Look for Real Synergy with Other Network Members***

In the legal profession, and in maturing markets for other professional services as well, networks of groups of members should be able credibly to propose and efficiently execute projects together that none of them could perform individually. Synergy among network members can produce substantial financial benefits for smaller law firms, and can enable them to compete successfully against their much larger, better-resourced rivals, especially on a regional basis. This is one area in which multi-disciplinary networks that cut across professional boundaries might have an advantage over general law firm networks or ones that specialize in a single practice area. Thus, synergy is emerging as a force that often can level the playing field between the global giants and local firms.

However, real synergy must be embedded in the way that a network operates and manages the risks of competitive disloyalty. Do members feel that the network understands and supports their strategic and business goals? Does the network understand the member's competitive context and strategic objectives, and take every reasonable opportunity to support the member? Do the actions of the network demonstrate that it has the interests of each member at heart?

***Pursue Expanded Referral Potential***

Most law firms join networks to gain referrals that they might not be able to obtain on their own. It is useful to conduct a little due diligence about the practices and client bases of other law firms in the network. Are they compatible? Realistically, how probable is it that they will actually send us work? One of the most important things that professional services networks should do for their members is to demonstrate, by simple and unequivocal metrics, the specific value of the referral potential of membership – practice area by practice area and jurisdiction by jurisdiction, if possible. This allows law firm partners to evaluate for themselves the probable return on investment.

***Consider the Network's Brand***

Most of the largest professional services networks work hard to develop a distinctive brand, often promoting that brand as a kind of "seal of approval" for their members. Although branding is not unimportant, being a member of a well-known network does not, by itself, transfer competitive advantage to a law firm. Sophisticated purchasers of legal services, especially in-house counsel, base their decisions on factors that are more directly related to expertise and service quality. The most that the network affiliation does is to get a firm onto the list of candidates – and often not even on the "short list." For this reason, any marketing reference to a law firm's network membership must describe specific, tangible benefits that are important to the client and that are a result of network membership. An area in which network branding clearly can create competitive advantages for members is in the synergy that a network can generate, which in turn produces tangible client benefits, which a competitor might not be able to deliver as well, or at all.

***Leverage Networks to Bring Internal Value***

Most professional services networks and their members overlook the internal value of joining a network. Internal value, however, could soon rival and, in some instances, surpass the traditional assumption that the primary purpose of a professional services network is to produce more and better fees. Membership in a network has the potential to bring positive impacts on a law firm's bottom line by reducing overhead, improving the efficiency of core business and technical activities, and decreasing capital expenditures. For some firms, the benefits for internal value could be the compelling reason to join a network. This is especially true for three types of networks: (1) general practice networks with a regional focus; (2) general practice networks consisting predominantly of small or midsize members; and (3) specialized networks in areas such as tax or labor and employment.

Although internal value currently is a largely unknown concept for most networks and their members, law firms should consider to what extent professional services networks could help them to increase the productivity and profitability of their internal operations. Some examples of how shared infrastructures provided through networks could support substantial improvements in fee earner productivity, internal operating efficiency, and reduced operating costs include:

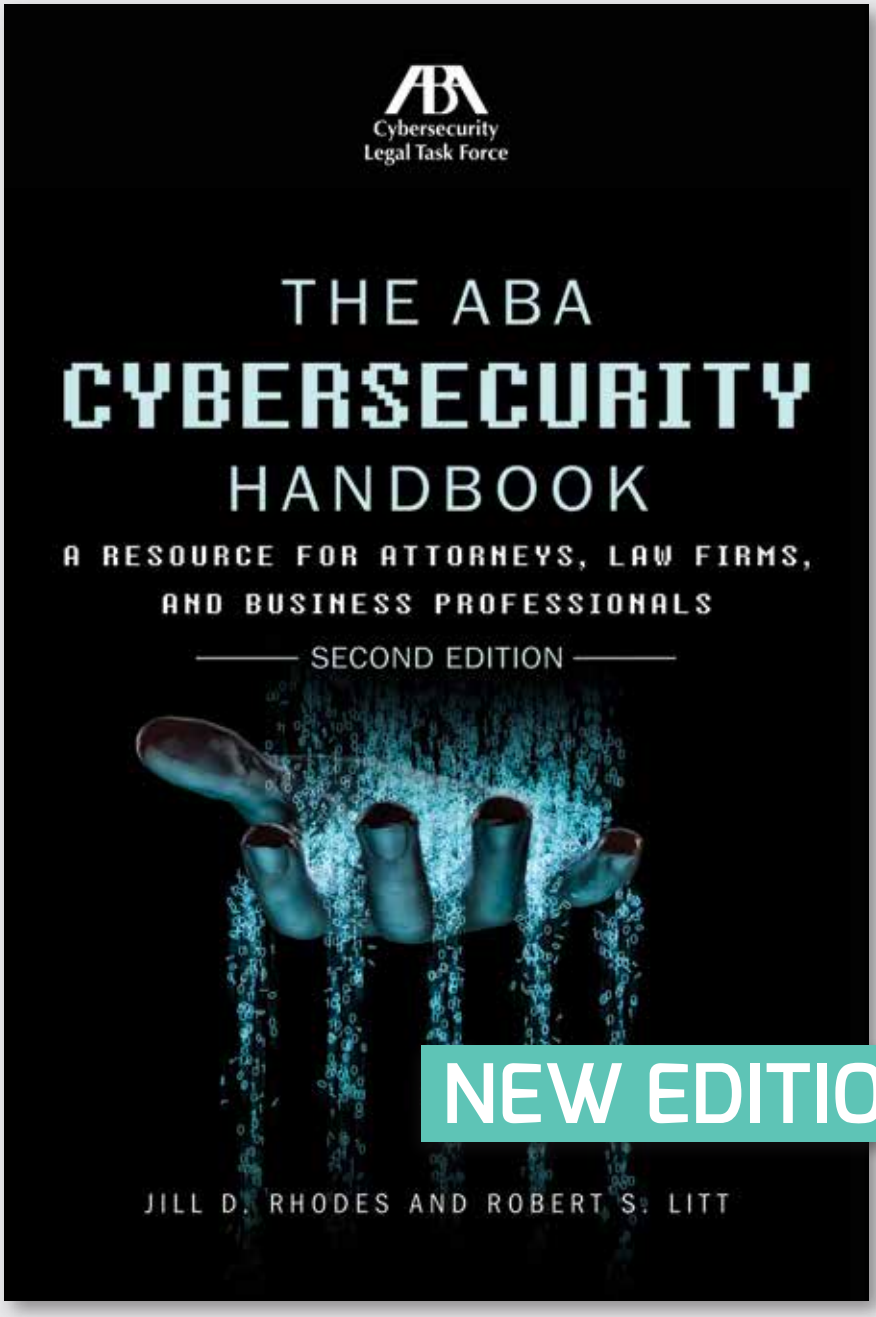
- knowledge management
- specialized information technology applications
- client relations management
- quality assurance
- financial management and reporting
- human resources administration
- information security
- premises security

Possibilities such as these imply a substantial shift in paradigms that have traditionally governed the perceptions of the purpose and value of professional services networks. The paradigm of external value is shifting from being focused primarily on referral potential to the possibly decisive importance of synergy. Thus, networks and their members need to expand their thinking about internal value as they move forward together in this era of unprecedented change in the legal profession.

## How Can My Law Firm Succeed? Compete More Intelligently!

So, what should a local law firm do when an international giant comes to town? Compete more intelligently. What does competing more intelligently mean? It means understanding what will be the successful competitive strategy for your local firm in a legal market that

*continued on page 40*




The Second Edition of this top-selling cybersecurity book is a must-read for anyone working in the field including private practice attorneys and associates, in-house counsel, non-profit and government attorneys and others.

Since the release of the first edition published in 2013, cybersecurity breaches in law firms have made news headlines and clients are asking questions about lawyers' and firms' security programs. From the massive Panama Papers breach that led to the dissolution of the Mossack Fonseca Law Firm in April 2016 to the WannaCry and Petya Ransomware attacks, the latter that led to the several day work outage at DLA Piper in June 2017, it is imperative that attorneys understand the potential risk of weak information security practices to their practices and their clients. As hackers increase their capability to conduct cyber attacks, so must law firms step up their risk management game specifically in cybersecurity as a fundamental part of their sustainable business practices.

Co-edited by cybersecurity leaders, Jill D. Rhodes and Robert S. Litt, former General Counsel of the Director of National Intelligence, The ABA Handbook on Cybersecurity, Second Edition focuses on many of the issues raised in the first edition, while highlighting the extensive changes in the current cybersecurity environment. Aside from the length of the book (about 30% more extensive than the prior edition), this edition includes a chapter on technology basics for the technologically challenged.

This updated book will enable you to identify potential cybersecurity risks and prepare you to respond in the event of an attack. It addresses the current overarching threat as well as ethical issues and special considerations for law firms of all sizes. The Handbook also includes the most recent ABA Ethics Opinions and illustrates how you should approach the subject of cybersecurity threats and issues with clients as well as when and how to purchase and use cyber insurance.

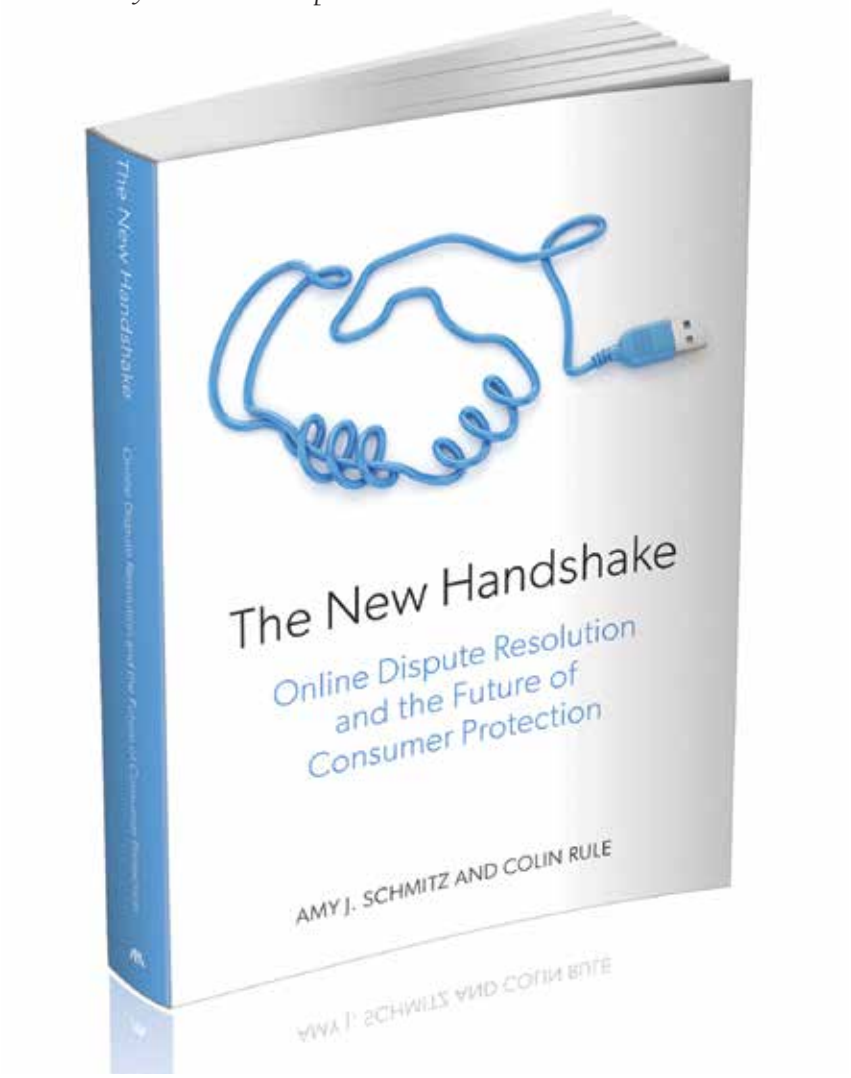
*2017, Paperback, 6x9, PC 3550028*
General Public $89.95
**ABA Members $71.95**

**ambar.org/cybersecurity**

# BOOK REVIEW

## *The New Handshake: Online Dispute Resolution and the Future of Consumer Protection* by Amy Schmitz and Colin Rule (ABA Publishing, 2017)

*Reviewed by F. Peter Phillips*




For many years, a tempest has surrounded public-policy approaches to consumer protection, largely implicating three utterly inapt legal constructs: FRCP 23, the Federal Arbitration Act, and traditional principles of contract formation. Accustomed to managing customer complaints but unwilling to expose themselves to the coercion of class actions, companies have sought to require consumers to waive rights to collective remedies. Courts have recognized the validity of contracts containing such waivers if they are embedded in agreements to arbitrate. And consumer agreements to arbitrate have been enforced regardless of whether consumers knew that they were agreeing to anything, what they are agreeing to, or what rights they were waiving.

So intractable has been the legal discourse that Congress, through Dodd-Frank, created an agency to promulgate rules protecting consumers of financial products from "forced arbitration and class action waivers." So vulnerable is our public policy to political change that, upon the ascendance of the Republican administration, that promulgating agency (the Consumer Financial Protection Bureau) and its proposed rules are likely to be stalled or overturned.

This climate has been a testament to the futility of the law to address a social need in a way that conforms to consumers' legitimate expectations.

Now come Prof. Amy J. Schmitz of the University of Missouri and Colin Rule of Tyler Technologies with an extra-legal, market-driven, empirically based approach whose values, they convincingly argue, reflect "old-time America" and yet whose execution relies upon cutting-edge technology. Illustrating old-time America, Professor Schmitz remembers when she would buy ears of corn from a local farm stand, hand the farmer a buck, and shake his hand. The dollar signified the market value of the corn, while the handshake signified the farmer's willingness, in the event that an ear was wormy, to replace it with a good one.

President Harry Truman expressed his frustration with economic advisors who equivocated "On the one hand . . . but on the other hand . . ." by declaring that what

**F. Peter Phillips** is an arbitrator and mediator practicing through Business Conflict Management LLC in Montclair, New Jersey. He is also the director of the Alternative Dispute Resolution Skills Program at New York Law School where, as an adjunct professor, he teaches Alternative Dispute Resolution, Negotiation, and International Commercial Dispute Resolution.

this country needs is a one-armed economist. Schmitz and Rule suggest that what this country needs is a "New Handshake." Their book of that name, published in April 2017 by the ABA Section of Dispute Resolution, makes a compelling argument.

For new technology, the authors explain the legitimate expectations of online retailers and their online customers. Both seek, and almost always realize, accuracy, satisfaction, efficiency, and responsiveness. Retailers devise easy methods of product identification, ordering, payment, and order fulfillment. Moreover, they compete with others in the marketplace to provide those experiences better than their customers' alternative suppliers. Consumers want ease of use, quick delivery, conforming goods, and both privacy and safety with respect to the details of their financial transactions.

The question is, if most of those online transactions go as contemplated, what do consumers expect with respect to the few that do not? And what are the market justifications for retailers' trying to meet those customer expectations?

Rule and Schmitz argue that the nature of online transactions presents the opportunity for the management and resolution of consumer disputes online, presenting opportunities for both customer satisfaction and enhanced business. Setting aside the concerns of third-party advocates, regulators, and lawyers, the authors propose that what customers really want is a dispute process that is as easy to access as the sale was; is online, like the sale was; and is fair, quick, private, confidential, effective, and direct. They do not want coupons, negotiations, arguments, excuses, or offers of discounts for future purchases, and they certainly do not want to have to pick up a telephone and have a recording tell them how important their call is.

Here comes the most compelling part of the authors' argument: based on a study of the buying behavior of millions of consumers on the retail site eBay, the authors conclude that consumers who are offered, and who initiate, online dispute management processes concerning their purchases actually engage in more purchases—irrespective of the outcome of the dispute process they initiated. That is to say, the mere availability of direct, simple online access to remedy boosts customer loyalty with respect to that online merchant. The authors even call this phenomenon "Return on Resolution," or "RoR." Return on resolution can backfire if done badly, of course. If the online consumer redress protocol is perceived as unfair, complaints get lost, or other adverse experiences lead customers to feel hoodwinked, things will change rapidly for the worse. But the empirically based proposition is that the presence on a retail website of an online consumer dispute mechanism results in enhanced customer loyalty. It acts like a farmer's handshake.

If the validity of this consumerbehavior, not self-described consumer "satisfaction," is accepted, then a whole new world of online dispute resolution presents itself, driven and enforced by the market rather than by legal theories or regulatory initiatives. The authors envision a global, uniform, multilingual, cross-cultural system of online consumer redress that possesses certain design criteria:

- The process is easy to access and to understand;
- The system is highly automated;
- Users of the process are treated fairly and their privacy is respected;
- The system identifies "bad guys"—fraudulent sellers and repeated claimants—and uses a "tripwire" system to exclude them from participation or notify appropriate authorities;
- The process is sufficiently sophisticated to detect other efforts at "gaming;"
- The process must yield benefit to the merchants who take part; and
- The system must self-improve through iterative lessons learned.

They go on to spell out in some detail how such a global network might be built on a single platform. And they offer hypothetical case stud-ies of how it would work in instances of buyer nonpayment, seller failure of delivery, dissatisfaction with quality of service, or other common business-to-consumer disputes.

These are timely, innovative, creative ideas. And it is a refreshing reminder that the law follows, and seldom incites, human endeavors. New developments in trade relationships come from the felt needs of the market, and when the market undergoes fundamental reshaping www.newhandshake.org such as the multijurisdictional, multilegal, cross-cultural, clickable world of con-temporary online retailing—we lawyers are fortunate to have people like Amy Schmitz and Colin Rule to point us to the leaders and encourage us to follow.

**Find this book and many more at www.ShopABA.org.** ◆

# Lessons from the Internationalization of Chinese Law Firms

*By Asen Velinov*

Each consecutive year in the last decade has been a record one for Chinese outbound investment. Even with the relative slowdown in activity in the first months of 2017, China work is still on everyone's radar—virtually every law firm in the world that has meaningful international practice wishes to participate in the action. As China's consumers, entrepreneurs and enterprises have developed an appetite for foreign products, travel and targets companies and the government has made it a key objective to encourage "Going Global," understanding the driving forces, motivation and key factors of internationalization of enterprises and service providers is key to being prepared for Chinese clients and working on transactions with Chinese lawyers.

At the same time, some foreign firms that have had presence in China for a long time, have recently left the market—inbound business volumes have decreased significantly—what makes "business sense" for enterprises, domestic and foreign lawyers and law firms in this new and complicated environment would often vary—and there are numerous soft factors to consider when going regional, international, and especially when "globalizing."

Recently, I helped produce a short series of interviews on the internationalization and international business of Chinese law firms for the show "Going Global" on the Shanghai Media Group (SMG) Oriental Financial Channel, with host and producer Lin Ying. The firms we covered are some of the most representative in the Chinese legal industry. They are all firms with over a thousand lawyers, with Dacheng Dentons being the largest law firm in the world by headcount. They are all the type of firms that large Chinese corporate clients go to for assistance with outbound inquires, plans or transactions (which often means more than strictly traditional law firm services).

Within this group, there is a notable absence—that of the arguably most international Chinese law firm—KWM. As we produced the series the firm was going through a "restructuring" of its European practice and did not accept our interview request. Their collapse in Europe is now seen as a case study of inadequate law firm management, even by the firm's own new global managing partner.

Understanding how Chinese law firms work also helps understand how Chinese clients approach their international deals, and working with Chinese firms is, for many firms without China presence, the only way to get large Chinese corporate clients (and might be a better approach than establishing presence in China due to both complicated regulatory environment and cultural barriers). Understanding also that often there are no clearly defined strategies for approaching international work in China can be of value to international lawyers who wish to work with Chinese colleagues; there are many stakeholders, "soft" factors (e.g., branding) and purely domestic reasons to internationalize for both enterprises and law firms. Moreover, even if 2017 has seen a slowdown of outbound activity directly out of China, the fact is that after more than a decade of unprecedented activity there are lots of Chinese assets overseas now (i.e., Chinese money is more reasonably "reachable" through foreign courts), which would inevitably lead to changes in how Chinese clients approach future deals, further internationalization strategies and risk management.

On January 9, 2017, the Chinese Judicial Bureau, the Ministry of Foreign Affairs, the Ministry of Economics and the Legislative Affairs Office of the State Council of China jointly issued the "Opinion on the Development of International Legal Services," which "encourages and supports the internationalization of the legal industry, legal talents and professionals, so that they can complement the "Going Global" efforts of Chinese investors and enterprises." Against this background, and that of the Belt and Road initiative, we look into the internationalization of Chinese law firms.

In recent years the Going Global efforts of Chinese enterprises have become an inescapable topic of discussion. Enterprises "go global" in accordance with their strategies and in search of international opportunities and partners.

Such enterprises naturally encounter legal issues; helping resolve those is the key role that law firms play in the "going out" era. At the same time, law firms themselves have joined the "going out" wave. We will introduce the specific approaches to internationalization of some of the leading Chinese law firms.

The internationalization of Chinese law firms is influenced by various factors such as their specific characteristics, the legal practicability of internationalization, customer needs and future plans, and is still in its infancy in comparison with some foreign law firms that have had international presence for much longer.

## Junhe Law Firm Managing Partner Xiao Wei

Junhe Law Firm is considered the first Chinese law firm to "go global." It set up a New York branch in 1993, and, after years of international practice, integration of resources, a carefully planned long-term growth strategy, and the creation of mechanism to ensure and maintain

**Asen Vilenov** (*asen@co-effort.com*) is an attorney-at-law in California; International Counsel at Co-Effort Law Firm, Shanghai, China; and a consultant, Shanghai Media Group, Oriental Financial Channel in Shanghai.

quality of services, has established its own approach to internationalization.

***What is the internationalization model of Junhe?***

***Xiao Wei:*** *Our internationalization approaches vary. We establish various types of cooperation with leading law firms in their respective jurisdictions. One approach is participation in legal networks, another is establishing "best friend" relationships, especially with prominent Asian and European law firms. After our respective teams cooperate on a number of deals, we include the firms in our "Best Friends" network. That is naturally not enough, as clients and their requirements vary (for smaller transactions we need to identify smaller firms), and they are not necessarily included in our networks.*

*In the best friend model, the key is meeting client needs, that's why flexibility is its key characteristic. In this type of cooperation, during actual projects the cooperation is close, and, after the project or case are completed, the firms return to a "friends" status until the next project. Contracts that protect the clients and their interests are the norm, so the cooperation on particular transactions is always contractually regulated.*

*Junhe's service model has been tested in more than 20 years of practice, from the help the firm has given SOEs with their overseas bond issuing, real estate acquisitions, and listings of pharmaceutical companies. In addition to the "best friends" model, Junhe is also a member of a number of international networks like Multilaw and Lex Mundi and has cooperation law firms in the United States, Italy, and Denmark that have positioned it well to help clients with their international M&A needs.*

***Junhe has helped numerous enterprises with their international transactions, what are some suggestions you would give to enterprises from the perspective of risk management of such transactions?***

***Xiao Wei:*** *Labor issues are a very important consideration, and often they are not given enough attention. Often the management team will be local (non-Chinese) and that leads to various complications and cultural issues. This requires sufficient legal preparation and attention. Another issue is that Chinese companies are often too eager to invest abroad; they are anxious to pick targets and complete deals, without giving much thought to postdeal integration and other subsequent issues.*

Chinese companies that "go out" need to address the realities of different legal systems and all resulting risks and challenges. Undoubtedly, law firms play a key role in managing such risks, but the legal industry of China is itself relatively young. Chinese law firms are mostly of two categories: corporate management model and pure partnership model. Junhe is a firm in the first category, meaning that the management and decision-making when it comes to the structure, strategy and development of the firm are centralized. Client resources are also more centralized in corporate model firms, while in the second type of firms, they would be held at individual partner level. Internationalization approaches vary between these two types of firms.

## Dacheng Dentons Senior Partner Wu Ming

***Wu Ming:*** *Internationalization has always been of key importance to Dacheng from the very beginning. We use three models: first, establishing overseas offices, second, membership in organizations like the World Services Group, and third, our current most important model, a Swiss Verein structure with Dentons.*

*International nonprofit organizations such as the World Wildlife Fund, FIFA, and also professional organizations, such as Deloitte & Touche LLP, have adopted the Swiss Verein model. The key characteristic of this structure is that its members are financially independent, and management is on regional level. For example, North American has a North American management team, Asia has an Asian management team and every member is subject to the laws of its own jurisdiction. Within the alliance, the members share a brand and work together on strategy and marketing. There is technological integration too.*

***Within such a large global team there are numerous nationalities and lawyers and support staff from various backgrounds. How do you deal with the cultural differences?***

***Wu Ming:*** *Because Dacheng itself in China and is managed locally, there is not much of an issue, when it comes to the different cultures between the different centers, we retain our culture and work together to give value added services to our clients. I think that our commonly shared principle is that working together is like making a bigger cake, and, in turn, each of us ends up with a bigger case from that bigger cake. That is more important than focusing on splitting a smaller cake very fairly.*

Internationalization has been a key focus of most Chinese law firms in recent years, and how the differences in legal systems, cultural and educational systems affects the process is of key importance to the management teams. The need to compete internationally and for client resources has greatly sped up the process of internationalization despite the inevitable complications.

***Please give us an example from practice, when a large Chinese enterprise "went global," via a merger or an acquisition. Was the foreign firm or Dacheng in a more dominant role?***

***Wu Ming:*** *Recently, we are more inclined to take the dominant role when Chinese enterprises go global. Our advantage being that we understand the client needs best, and we can convey their needs and intentions to our foreign colleagues better. We can also help the client understand better the important factors and considerations and help all sides discuss and reach a decision on strategy. This role is actually the dominant one.*

It is important to note that firms in Swiss Verein structures have

experiences some problems, usually financial and operational ones. Also, it seems that there are gaps in the level of professionalism between the Chinese and foreign teams, which leads to communication problems, e.g., in the use of standard documents and an uniform database. There appears to be room for improvement of the model.

### Yingke Law Firm Director Li Judong

The "best friends" model adopted by Junhe Law Firm is about working with elite overseas law firms. In short, similar to a relationship between friends, it boils down to contracting for specific projects, and remaining "friendly" while not in touch; while Dacheng's Swiss Verein approach allows the shared use of a brand while remaining relatively decentralized. Let us next explore what the model of Yingke law firm is, and how it fits within the Yingke group of companies.

Beyond the original legal platform, Yingke has extended its services to include travel, education, immigration and other services, packaging its services in a "one stop shop." The firm has established overseas offices and the Yingke China Center, and we will now discuss the Chinese style internationalization of the firm.

***Li Judong:*** *The purpose of our branch offices is primarily to provide legal services, and the purpose of the China Center is to provide what we call "one stop" business and legal services. When a Chinese enterprise goes global, it would need more than just legal services; it needs general business services, like information about the investment environment of the desired country, project selection, management services postdeal, including labor resources, communication services, etc. Many of these do not strictly fall under the scope of pure legal services.*

*As a Chinese law firm with the largest number of lawyers in the Asia-Pacific region, Yingke's one-stop business legal service platform deviates from the definition of traditional legal services provider. Their services extend to project matchmaking, management, consulting, etc. This comprehensive model is more suitable to Chinese investment approaches. Yingke does not only assist enterprises in their "Going Out" but also plays role in collecting, matching and integrating foreign resources. Aiming to provide comprehensive internationalization support, Yingke has itself comprehensively internationalized.*

Whether it is the road of internationalization of Chinese law, or the adoption of a common international model, local bar associations are important participants in the internationalization of Chinese law firms and play a significant role in it.

### Shanghai Bar Association President David Yu

***David Yu:*** *To enhance the ability of the lawyer to provide international related services, we often host trainings by internationally recognized experts, lawyers from international law firms and academics who visit to talk about different aspects relevant to servicing the companies that are "going global." We would also sometimes choose promising excellent young lawyers and arrange internships, secondments or positions for them in prominent law firms abroad. We can say that the lawyers able to provide international services is constantly increasing.*

As the Chinese economy inevitably becomes more integrated into the global system, the development and internationalization of the Chinese legal industry deserves our continued attention.

Junhe's "best friends" model, Dacheng Denton's Swiss Verein, and Yingke's "one stop shop" international legal services" model are uniquely suited to each firm's characteristics and objectives. Yet, all of them, as well as the other top Chinese firms continuously explore options for adjusting and improving their internationalization approaches.

### Tahota Law Firm Partner Li Jinnan

On December 18, 2015, Tahota Law Firm held an opening ceremony for its office in Washington, DC—the first such office for a law firm from the western part of China. It also marked the beginning of the firm's internationalization.

***Li Jinnan:*** *We first opened an office in DC, and at the beginning of this year the opening of our offices in Seoul and Busan was approved by the Korean Ministry of Justice. We are in the initial stages of exploring internationalization. In accordance with China becoming a more integrated part of the global economy and especially in the time of the Belt and Road strategy, an increasing number of Chinese enterprises "goes global." As a result, they need a more international vision, and need experienced legal teams to help plan their international strategy. The law firms themselves also seek to internationalize, in order to strengthen the quality of their services.*

***Is it accurate to describe the internationalization strategy of Tahota as one focusing on primarily establishing overseas offices?***

***Li Jinnan:*** *This is an important part of our strategy. As I mentioned, we are in an exploration stage—opening overseas offices comes with various considerations, such as different requirements and a different legal environment. The concrete location dictates whether to set up an office, or to enter into a cooperation with an existing office and at an appropriate time in the future discuss a more comprehensive cooperation or a merger.*

Facing an unfamiliar overseas market, Tahota has clearly positioned its DC office; it serves as a "window" to facilitate the hiring of international lawyers, optimizing communication with local resources and better meeting the needs of clients in the western China, thus making the firm more competitive in its region. With its services being more competitively priced than those of international firms, Tahota also better meets the needs of the clients in western China.

***Li Jinnan:*** *Establishing foreign offices brings about risks to the entire firm, as various issues at the location of the overseas office could affect the entire firm and its reputation within China, thus for us risk management is key during the process of our internationalization. As we focus on the development of a long-term strategy, we do*

*not exclude the possibility of establishing close cooperation with overseas law firms.* Apart from TAHOTA's internationalization through the establishment of foreign offices, there are other models that Chinese firm explore as they try to find one that is optimal for their specific needs and capabilities. One of the oldest full-service law firms in China, Zhonglun has numerous practice groups and a very cautious approach to internationalization.

### Zhonglun Law Firm Partner Yang Wantao

***Yang Wantao:*** *Zhonglun has tried different models in the past, at different stages of our development. Zhonglun as a full-service law firm, with a client base that is also very large and varied, different client groups have different needs, so we aim to be flexible, to consider all the appropriate opportunities and structures, and we have different models for different practice groups and client needs.*

The international market offers a couple of approaches to internationalize, one is the Swiss Verein Structure; the second is the "Best Friends" model; the third is to set up overseas branches. These models are different, and in order to maintain its flexibility, Zhonglun has not committed fully to either one of those, instead searching for its own, special internationalization model.

***Yang Wantao:*** *The Swiss Verein structures leads to the formation of a large-scale union of firms, where the local members are relatively independent, which minimizes risk and responsibility, but leads to often inadequate integration.*

The Swiss Verein model is at present the most commonly used model in the internationalization of large-scale law firms at present. This model can quickly establish a large legal network relationship and provide a platform for resource sharing. The members retain relative independence and have the ability to manage their risk within the larger organization. However, in the separation of management, profits and the fact the members are in jurisdictions with different regulations, leads to various issues like competition for client resources.

The "Best Friends" is also a model commonly used by international law firms. It comes with no legal obligations and is the formation of a "friendly" relationship through "friendly" cooperation. Law firms typically choose to cooperate with similar other firms, thus reducing communication barriers. During the duration of specific cases of cooperation is governed by a contract, and the rest of the time the firms retain full independence.

***Yang Wantao:*** *According to my understanding, the "Best Friends" approach is motivated not by the actual search for "friends" and applies usually to smaller, specialized firms, as they are smaller, their client needs are also specialized and this approach typically does not lead to forming large global networks.*

Compared to the first two models, the establishment of overseas branches is another simple and efficient internationalization approach. The overseas

establishment of the branch office model can directly carry out international business development, and as Chinese enterprises go global, many Chinese law firms choose this approach.

***Yang Wantaot:*** *Establishing a small foreign office is a quick and cost-effective way to meet short term needs and establish presence. However, in countries with mature legal systems, local competition is intense and local firms provide competitive services for large-scale projects, which makes it difficult for smaller Chinese law firm offices to compete for such projects. And, if such offices are established for only a short period, acquiring and retaining talent is an issue. In Zhonglun we don't have a rigid model or a fixed approach.*

At this stage, most Chinese law in the process internationalization, while also still in the stage of exploration and selection of their own model. As an important window for opening up, in 2014, the Shanghai Pilot Free Trade Area under the Shanghai Municipal Government issued the "Notice of the General Office of the Shanghai Municipal People's Government on Forwarding the Implementation Measures for Mutual Assignment of Lawyers to Serve as Legal Consultants by Chinese and Foreign Law Firms in China (Shanghai) Pilot Free Trade Zone and the Implementation Measures for Economic Association between Chinese and Foreign Law Firms in China (Shanghai) Pilot Free Trade Zone Developed by the Shanghai Municipal Bureau of Justice." These regulations allow Chinese and foreign law firms to coordinate sharing human and other resources, cooperate on providing legal services and other relevant projects. They also allow Chinese and foreign law firms in the Shanghai Free Trade Zone to form joint ventures. At present, Baker & McKenzie and Fenxun Law Firm have set up a joint office in the Shanghai Free Trade Area to deal with international and Chinese legal affairs. The internationalization model of joint ventures between China and foreign universities is still in the first stages and perhaps will prove to be a worthwhile one.

No matter what exact model they choose, Chinese law firms are well on the road to internationalization. Legal talent is one prerequisite for internationalization and it appears that its internationalization also has room for optimization.

## Shanghai Jiaotong University Koguan Law School Vice Dean Yang Li

***Yang Li:*** *It should be said that in the past decade, Chinese law education has entered a period of a "Great Leap Forward", but this period has had two downsides, the first is oversupply, the second has to do with structural issues. The main reason is that there is sufficient number of junior legal talent, with grasp of foreign laws, foreign languages, foreign culture and cultural differences, as well as experience with international enterprises and firms, but what is lacking is more senior talent with sophisticated foreign legal experience.*

Colleges and universities are constantly striving to improve the cultivation of legal talents.

***Yang Li:*** *According to the system of the ministry of education, top tier universities should be training lawyers to engage in diplomatic affairs and to be able to represent China's national interests in the international arena. Some financial and trade, focused universities, as well as language college graduated, after having received a systemized practical-focused education, would benefit from training in our law school, for example.*

In addition, universities close to national borders naturally establish exchanges and cooperation with foreign universities in their regions. SJTU cooperates with the Shanghai government, numerous social and business organizations and foreign lawyers in order to train stakeholders so that they are ready to engage in foreign related legal affairs and projects.

In recent years, due to the internationalization of law firms in China law more and the proliferation of foreign related business, in addition to those Chinese legal talents with overseas experience, many foreign lawyers are more attracted to the Chinese market, the status of foreign legal talent in China should also be discussed.

## Foreign Attorney Asen Velinov

***What's the role of foreign lawyers in the process of Chinese enterprises "going out"?***

***Asen Velinov:*** *"Foreign" lawyers play an important role in the process of "going out" of Chinese enterprises. When Chinese enterprises engage in overseas investment, most of the drafting of documents is actually done by "foreign" lawyers (who are at that point "local" lawyers in the target jurisdiction). Foreign lawyers themselves have communication advantages, and many (of us) foreign lawyers working in China believe that we should be more involved in these processes. And as culture is more important than language skills when it comes to successful deals, foreign lawyers with Chinese backgrounds are more able to add value more in this respect than many Chinese lawyers. When foreign lawyers are a part of the legal team of a Chinese law firm, such a firm can better serve their clients and clients should take this into account when choosing a domestic team of lawyers to provide international legal services for them.*

Whether it is Dacheng Dentons, Junhe, Zhonglun, Tahota or Yingke, these leading Chinese law firms, with their approaches to internationalization, they are also in constant search of ways to optimize and fine tune their approach, not just cautiously exploring their internationalization strategies but constantly adjusting their approaches. ◆

# How American Attorneys Can Make a Local Practice outside of the United States

*By James A. Nickovich*

Many American law students dream of working in Europe. Seasoned attorneys crave for a few years in Asia. A spouse's career may necessitate an international move for the family. Practicing abroad is a romantic proposition, but few American attorneys make the move because there is no riskfree path. But if you are willing to be there, be flexible, and give, it can be done.

## Be There

Countless attorneys would love to live in Zurich (or Rome or Buenos Aires) and express their interest by e-mailing local firms' hiring partners, to no response. If you knock on that hiring partner's door, you will get more attention. There is no substitute for presence; having mastered a few basic local phrases and with a letter of recommendation in hand.

## Be Flexible

It is unlikely that you will be admitted to the local bar in your new home, foreclosing aspects of your prior practice (e.g., pleading in court), but this can be an opportunity to learn something new. Many litigators have happily crossed into arbitration, never to return to court.

## Give

### *Substantive Knowledge*

The U.S. attorney-client privilege impacts foreign lawyers, though most know little about it. Civil law attorneys can be puzzled by America's voluminous discovery obligations, and have less experience conducting cross-examinations than American practitioners. Make a presentation on such topics to everyone in your new firm. Not only will this lead to opportunities for you inside the firm, but it can also open doors for you to provide similar talks to firm clients and external groups in your new country. While you may not feel like an expert, as the American in your new firm, you are the American legal expert. And you will earn that title. Few tasks develop competence quicker than explaining complex new concepts to a room full of lawyers.

### *Language Skills*

Law firms abroad all conduct at least some business in English and you may be the sole native speaker in your new firm. When there is a lot on the line requiring the perfect English phrase, sentence, or contractual clause, everyone in your firm should feel comfortable running drafts past you.

### *Intermediary Abilities*

While you will be the "American" in your new firm, you may also be the only American attorney that your former U.S. colleagues know where you now live. This means reduced competition for particular types of matters. Your foreign firm may need to refer matters into the United States and look to you for leads or managing such referrals, while your former U.S. co-workers may need guidance on an issue in your new land. Instead of the typical model of competing with countless similarly situated attorneys in the same hometown, under your model as an American attorney practicing abroad, you are the natural—and perhaps only—intermediary for matters that touch both of your "two worlds." Step into this role and work on the cases you can handle, while taking advantage of the introductions and referrals you can make. Your colleagues from both worlds will appreciate it. ◆

**Jim Nickovich** (*jnickovich@vischer.com*) is counsel for VISCHER AG, based in Zurich and Basel, Switzerland, focusing on international arbitration. He previously spent a decade with two law firms in San Francisco litigating in state and federal courts across the United States. He participates in the Section's International Arbitration Committee and International Anti-Corruption Committee.

# Statement on the Passing of Professor M. Cherif Bassiouni

***A founding member of the ABA's ICC Project Board of Advisors, Prof. Bassiouni's positive impact on the field of international criminal law is immeasurable.***

Professor M. Cherif Bassiouni, who passed away September 25, was a true giant of international criminal law, or as many called him, its "father." His contributions to increasing criminal accountability for mass atrocity crimes in particular, and to the advancement of human rights in general, are legion, and they will endure. His career was unparalleled in many respects and recounting his accomplishments is almost impossible to do (*The Washington Post* did an admirable job attempting to do so). His professional contributions were matched by his good humor and his openness to engage with anyone, be it a president of a nation or a first year law student.

Prof. Bassiouni was an active and influential member of the American Bar Association. He was one of the first members of the Board of Advisors of the ABA's International Criminal Court Project, and stalwart supporter of its initiatives. He was also a driving force behind the formation of the International Criminal Justice Consortium that the ABA and Siracusa International Institute (which he founded and served as its president) are members of along with twelve other rule of law and human rights organizations. We will miss him deeply, and carry on our work that he will continue to inspire.

His contributions to increasing criminal accountability for mass atrocity crimes in particular, and to the advancement of human rights in general, are legion, and they will endure.

*ABA–ICC Project*

# Year-End Reflections from 2016–2017 Section Chair Sara Sandford

**Sara Sandford** (*ssandford@gsblaw.com*) is an owner in the Seattle office of Garvey Schubert Barer and and served as Chair of the ABA Section of International Law 2016–2017.

In concluding my year as 2016–2017 Chair of the Section, I want to first thank all of you for the honor and privilege. It has truly been a year filled with challenging and rewarding experiences that I will not forget. The Section does so much great work, and you all make it possible. As I have said on a few occasions, it is remarkable to think about the dollar value of all the volunteer time that is spent on our Section's work—work that benefits us all.

This includes our programs and publications, of course. We have put on hundreds of hours of programs on a wide array of topics at several different events this year. Most recently, we held a free teleconference offering a broad view of expert opinions on the state of the legal system in Turkey, a year after the coup. It was attended by over one hundred people and offered an up-to-date picture on the legal aspects of the situation that one could not find elsewhere. We have published everything from a Chinese dissident's memoir, to newsletters, to a very comprehensive year-in-review volume, to scholarly articles in the International Lawyer. It was great to celebrate the International Lawyer's 50th anniversary this year! Our work has moved the practice of international law forward on both the public and private law front, as we educate, discuss, inspire, innovate and push for change.

We have also spent countless hours working on a variety of rule of law and access to justice issues. Most recent was our work on the ABA's statement raising concerns about a new law proposed in Poland. The law would have limited the independence of the judiciary. It is rare for us to know whether our efforts have an impact, but in this case Poland's President, who vetoed the bill, was reported by the New York Times as having been influenced by the ABA's statement. A few other highlights during the year were helping a wrongful charged attorney gain release from prison in the United Arab Emirates and the incredible teamwork displayed on our efforts on the U.S. President's Executive Order of January 27, 2017. We are fortunate to have a voice to support such principles throughout the world. We should continue to use that voice for the improvement of access to justice and the rule of law here in the U.S., as well as to support the efforts of our colleagues to promote similar principles around the globe.

I want to express special thanks to the leadership of the Section, who have worked so hard beside me this year: Steve Richman, the incoming Chair; Lisa Savitt, the Immediate Past Chair; Robert Brown, Vice Chair; Lisa Ryan, Secretary/Operations Officer; Joe Raia, Revenue Officer; Bill Mock, Budget Officer; Marcos Rios, Membership Officer; Nancy Stafford, Rule of Law Officer; David Schwartz, Policy and Government Affairs Officer; Patrick Del Duca, Publications Officer; Caryl Ben Basat, Technology Officer; Marcy Stras, Programs Officer; Yee Wah Chin, CLE Board Chair; Mark Wojcik, Diversity Officer; Ingrid Busson-Hall, Communications Officer; Renee Dopplick, Editor in Chief of the ILN; Lelia Mooney, Liaison Officer; and Beverly Duréaus and Patricia Heard, our two Co-Executive Editors of the International Lawyer. I would also like to thank our Senior Advisor, Mike Byowitz and our Delegates-at-Large, Jeff Golden, Glenn Hendrix and Gabrielle Buckley, along with our ABA Board of Governor's Liaison, Paulette Brown and our Legislative counsel of the GAO, Kristi Gaines. Your dedication and hard work throughout the year has been so appreciated and invaluable.

But our Section would not be able to do what it does without the fantastic staff we have: Leanne Pfautz, Section Director; Maria Chhabria, Associate Director; Thomas Happell, Senior Meeting Planner; Christina Heid and Somayina Boardman, International Projects Director and International Program Associate, respectively; Angela Benson, Membership Director; Sophie Wilmot, Committee Specialist; Samantha Feinstein, Sponsorship and Outreach Specialist; Jeanita Brown, Program Specialist, and Adam Vogel, Technology Specialist. I cannot imagine a harder job than trying to keep such a busy and complex organization running when many of the people providing you with input and help are volunteers! And often new to the work, at that! You all make it look easy, handling our requests and questions with such grace, good-nature and aplomb. I just cannot imagine how you do it!

We did not manage to accomplish everything I had hoped to this year, and there will always be more work for the Section to do to meet its members' needs, improve the profession and support access to justice and the rule of law. Still, I am so grateful for the opportunity to have worked with you all to accomplish what we did! We have a fantastic team of members, leaders and staff and the sky is the limit in the coming year, under Steve's able leadership. The ABA and the Section of International Law really are incredible avenues to improving our skills, knowledge and contacts and helping our clients, our communities and the world at large. I'm so grateful to be a part of it; thank you all! I look forward to seeing you at our next event. ◆

# Section Officers 2017–2018

## Executive Committee

*Chair*
**Steven M. Richman**

*Chair Elect*
**Robert L. Brown**

*Vice Chair*
**Lisa Ryan**

*Liaison Officer*
**Maximiliano J. Trujillo**

*Revenue Officer*
**Marcos Rios**

*Programs Officer*
**Marcela B. Stras**

*Budget Officer*
**William B.T. Mock, Jr.**

*Membership Officer*
**Patrick Del Duca**

*Immediate Past Chair*
**Sara P. Sandford**

*Secretary/Operations Officer*
**Joseph L. Raia**

## Administration Committee

*Rule of Law Officer*
**Mikhail Reider-Gordon**

*Policy/Government Affairs Officer*
**Kenneth N. Rashbaum**

*Publications Officer*
**Nancy Kaymar Stafford**

*Diversity Officer*
**Mark E. Wojcik**

*Technology Officer*
**Caryl Ben Basat**

*Communications Officer*
**David A. Schwartz**

*CLE Board Chair*
**Yee Wah Chin**

*Senior Advisor*
**Jeffrey B. Golden**

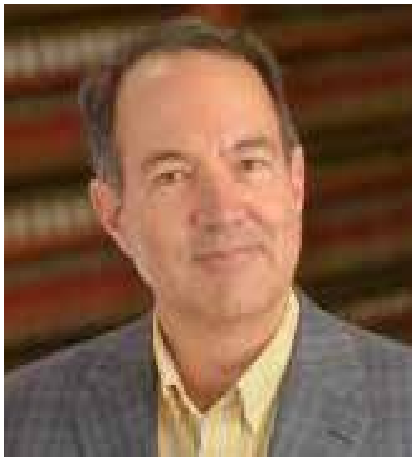
*Delegate/ Member-at-Large*
**Michael E. Burke**

*Delegate/ Member-at-Large*
**Glenn P. Hendrix**

*Delegate/ Member-at-Large*
**Gabrielle M. Buckley**

*ABA Board of Governors Liaison*
**Hon. Eileen A. Kato**

# Meet Membership Officer Patrick Del Duca



**Patrick Del Duca** (*pdelduca@zuberlaw.com*) is a partner at Zuber Lawler & Del Duca LLP and is the ABA Section of International Law Membership Officer for 2017–2018.

***As an experienced cross-border regulatory attorney, what do you love the most about practicing law?***

Creating solutions. Navigating, fitting together, and sometimes even reconciling apparently divergent bodies of law and ambitions of stakeholders provide intellectual and emotional satisfaction. Finance and technology are generally at the core of what I do, and much of my practice has a cross-border dimension to it. The individuals with whom I work are typically quite savvy, with distinct backgrounds and perspectives corresponding to their diverse professions and cultural backgrounds. Whether the underlying matter is transactional or adversarial, the privilege in this contextually rich workspace is to apply legal skills and knowledge in a sophisticated way to achieve value that did not previously exist.

***What was your first job after law school? How did that shape your career interest?***

Following graduation from Harvard Law School, I worked for a year as a clerk to Judge Alfred T. Goodwin of the US Court of Appeals for the Ninth Circuit. During that year, Italy's *Corte costituzionale* asked then Chief Justice Warren Burger for an introduction to an American law clerk. With Judge Goodwin's support (and having previously spent a year in Italy as a Fulbright Fellow), I was invited to the Supreme Court in Washington for interviews and then spent the following year in Rome as a law clerk to Justice Antonio La Pergola of the *Corte costituzionale*.

I did not complete my Ph.D. in law at the European University Institute in Florence until after that second clerkship, and completion of my Italian law degree from the Università di Bologna law faculty came two years later when I defended my thesis in Bologna, on a vacation break from practice in Los Angeles at O'Melveny & Myers, then Warren Christopher's firm

The judicial clerkship experiences in distinct legal systems at the elbow of deeply thoughtful judges offered me a valuable window into the world of advocacy, specifically the opportunity to assess from the vantage of the court what styles and qualities of advocacy were most effective. They also grounded me in problem-solving in each of the common law and the civil law traditions.

Both clerkships involved consideration of enduring issues with which I remain engaged. One particular fruit of clerking with the *Corte costituzionale* at a time when the relationship between European and Member State law demanded definition is an article co-written with Justice La Pergola (*Community Law, International Law and the Italian Constitution*, 79 American Journal of International Law 598 (1985)) and subsequently cited by the *Bundesverfassungsgericht* when it considered the issue in respect of German law: BVerfGE 73, 339 (*Solange II*).

***What initially drew you to become a member of the Section?***

About ten years ago as I contemplated the adventure of building my current firm, I chose the Section of International Law as my preferred international network. Having joined the Section, I found a unique and dynamic community of lawyers who share the convictions that our voices can contribute to further the rule of law, useful law reform, improvement of the legal profession, and enhancement of our members' careers.

It helped that within days of joining, Meaghan McGrath Sutton of our Section recruited me as a leader of the Mexico Committee, now one of our Section's most active. Collaborating to build that Committee cemented my commitment to the Section. Our team's focus on diversity was key, and is reported in Patrick Del Duca, Alejandro Suárez Méndez and Juan Carlos Velázquez de León Obregón, *The Mexico Committee–Nurturing Committee Activity and Diversity*, ABA Section of International Law Diversity Newsletter 7–10 (Fall 2012).

***What are you most passionate about in your role as Membership Officer?***

We seek to grow our Section's membership. Lawyer-to-lawyer, I am passionate to communicate the value–personal, professional and economic, that can flow from engagement with our Section. Within our Section, I am eager to encourage each of our members to invite a few friends to join. Our shared status as Section members empowers each of us to make new professional friends, inviting them to join us in Section activities. And, I seek to support the excellent work of our Committees across the board in recruitment and integration of new members, but especially of our Outreach Committee focused on new lawyers and law students. Among the excellent work of that Committee is our Section's Pathways program that recruits existing members to conduct outreach programs in law schools.

I am eager to communicate the many ways our Section's members step into the spotlight as part of advancing our Section's

work. Having just finished a term as our Section's Publications Officer, I mention a few opportunities in the publications field. Our Committees regularly publish newsletters compiled from timely, brief contributions by Committee members. Through our Committees' contributions to The Year in Review, an interested member can quickly be identified in a high circulation law review as the author of a short update on a legal development in the current year. Longer articles can be published in this *International Law News*, and full 10,000 work law review articles in our Section's flagship law review, The International Lawyer.

Although not every Section member will author a memoire such as that of Chinese human rights lawyer Zhisheng Gao (Unwavering Convictions, co-published by our Section this year with Carolina Academic Press), there are opportunities not only to author books and chapters of books that our Section publishes (e.g. forthcoming from the Mexico Committee in November is a multi-author work provisionally titled Mexico and its legal system: Lawyers' essays on the continuing evolution), but also to serve on the Section Books Board that oversees these activities. A similar richness of opportunities exists to contribute through each of our Section's sixty-some committees, multiple city chapters around the world, and activities focused on the breadth of Section meetings and programs, law reform efforts, rule of law initiatives, professional development, diversity and inclusion activities, etc.

### *Why would you encourage people to join the Section?*

Membership in our international community of lawyers opens many doors, including to:

- become a better lawyer,
- improve the law,
- advance a legal career,
- mentor others, and,
- make friends with a members of a community diverse in every way and united in an appreciation of the value of membership in our unique international legal community.

### *What do you like most about the Section?*

Our Section's members are spread across over 100 countries, yet our work is conducted with a sense of close community across boundaries of all kinds. Our members find leadership opportunities and visibility in our more than sixty committees (some focused on specific subject matters, others on a geography or other affinity) and our growing number of active city chapters. They likewise contribute in our Section's meetings of various sizes and focuses spread around the world as well as in our numerous publications (newsletters, law review and books) and policy and rule of law initiatives. We offer abundant opportunities to relate through both technology and travel.

### *What types of legal professionals are members of the Section?*

If you fall within our broad definition of a lawyer (no need to be a U.S. lawyer), we welcome lawyers globally–AND we welcome law firm lawyers, in-house counsel, government lawyers, judges, NGO lawyers, international organization lawyers, etc.–AND we welcome law professors and law students globally!). Join our community by becoming a member and encouraging your colleagues to become members. You may be surprised by just how economical it is to sign up (if you ask, you will learn about the ABA 50% discount promotion for new members of the ABA and our Section), but the true measure of your investment in our community will become apparent with time as you engage with us.

### *What types of trending and insightful legal information do members have access to?*

As a Section member, among the resources that you can access online, in addition to *International Law News*, is our flagship law review, The International Lawyer. In particular, you can read its volume 50(1), celebrating fifty years of its publication of the perspectives and insights of practitioners and scholars of our community. My own enthusiasm for what our members can achieve through our Section is laid out in one of its articles: *Why We Read The International Lawyer–Answers Parsed from Works of Two International Lawyers*, 50(1) The International Lawyer 87 (2017).

### *What are some ways that current members can help recruit new members?*

Surf the membership section of our Section website as a start to understanding the multi-layered opportunities to engage with us. As I can facilitate the process of engagement, please do not hesitate to reach out to me at: *pdelduca@zuberlaw.com*.

I hope to see you soon at a Section meeting, program, or event! ◆

# Meet Diversity Officer Mark E. Wojcik

**Mark E. Wojcik** (*mwojcik@jmls.edu*) is a law professor at The John Marshall Law School in Chicago and is the ABA Section of International Law Diversity Officer for 2017–18. He previously served as the Section Publications Officer. He is also a 2017–208 Fulbright Specialist at the Jigme Singye Wangchuck School of Law in Thimphu, Bhutan.

***You have a great deal of international experience working with a broad range of people from varied governance systems, legal structures, cultures, and societies. What have been some of your experiences?***

I clerked for the U.S. Court of International Trade and later served as Court Counsel to the Supreme Court of the Republic of Palau during the year that Palau became an independent country. (Before then, it had been a UN Strategic Trust Territory administered by the United States). I've taught at law schools in China, Lithuania, Mexico, and Switzerland and have been a visiting research scientist in Italy. My husband is from Italy as well—we met in Japan. I've also taught seminars and lectured in the Czech Republic, Egypt, Indonesia, Jordan, Singapore, and Turkey. I also organize the Global Legal Skills Conference in different locations around the world, including Costa Rica, Italy, Mexico, and next year in Australia.

***As a law professor, what types of international law resonate with you?***

I love being able to teach lawyers and law students how they can use international law in their domestic work. It's surprising how many lawyers are either unaware of applicable treaties or else don't know how to find out which countries are parties to a particular treaty or what reservations they claimed when they ratified the treaty. There's a lot of work to do with lawyers to teach them how to find and use rules of international law.

***Why did you decide to help open the first law school in Bhutan?***

**First entering class of the Jigme Singye Wangchuck School of Law in Bhutan**

It's an incredible honor to help launch the first law school in Bhutan, a small country sandwiched between its giant neighbors China and India. Bhutan transformed from an absolute monarchy to a constitutional monarchy only ten years ago, under the enlightened guidance of then-King Jigme Singye Wangchuck. The Bhutanese Constitution entered into effect in 2008. The law school is named after the former monarch. It is the first law school in the history of Bhutan, and it will train the future lawyers, judges, law professors, and other legal professionals that the country will need to implement that Constitution, ensure justice, safeguard fundamental individual rights, and uphold the rule of law. My husband and I worked there as Fulbright Specialists to help launch the law school. There are 25 students in the first class—13 women and 12 men—who will be the future leaders of Bhutan.

***What inspired you to focus on diversity?***

Diversity and inclusion are core values of the ABA and the Section of International Law. Our Section is probably the most diverse ABA Section because of our global membership—lawyers from so many countries, cultures, and backgrounds enrich our meetings, programs, publications, and activities. Look around the rooms of our section meetings and you'll see the world. We are truly enriched by the global diversity of our section, including diversity based on race, religion, gender, sexual orientation, gender expression, national origin, ancestry, age, disability, veteran status, marital status, or any other characteristic. We are diverse in the areas of our law practice: our membership includes judges, lawyers, in-house counsel, government employees, law professors, and law students. Also, who can count how many different languages are spoken at our seasonal meetings?

***How will the Section promote diversity this year?***

The Section has numerous diversity-related programming events. Many committees have Diversity Vice Chairs to help increase diversity at the committee level. The Section's new Diversity Fellowship Program, now in its second class of Fellows, has also brought a wide range of talented legal professionals to the important work of the Section. Through collaboration with leadership, diverse bar associations, and other ABA entities, we will continue to make great strides in our diversity goals. We're also working on a new five-year diversity plan for the Section.

***How can members become involved in the Section's diversity initiatives?***

I will be working closely with Division Chairs and Committee leaders to ensure that diversity is incorporated into all Section programming and meetings. Diversity and inclusion are at the heart of the Section

and finding new ways of reaching more diverse members is an important mission of the Diversity Committee.

If you have any questions or suggestions about how to promote diversity in the Section of International Law, please contact me at *mwojcik@jmls.edu* or contact one of the Deputy Diversity Officers. I look forward to working with you in the coming bar year. ◆

## Global Legal Market

*continued from page 24*

is internationalizing. Understand your firm's strategic path to profitable sustainability, its strengths, its differentiation in the marketplace, its specific value to clients, its business culture, and the drivers underpinning why and how you would change within the firm and externally.

Also, if you are a small or midsize firm, don't let the big guys scare you. From all the attention that "Big Law" is getting in the legal press and at legal conferences, one might erroneously assume that a relatively small number of large firms are destined to rule the legal world and that those smaller, local firms are irrelevant to the future of the legal profession. Don't believe it. Although being large can sometimes be an advantage, many small and midsize local firms are competing successfully, and will continue to compete successfully, for high-value legal work. The entry of large foreign law firms into a legal market is a challenge, but it also offers great opportunities. Merging with a larger international firm, or with another local firm, can be a good strategy for some law firms; but successful independence remains a financially viable option for others.

Merger or affiliation with an international firm will undoubtedly be a wise choice for some local and national law firms. However, there is, and will continue to be, a role for independent law firms in emerging and recently-emerged legal markets. The best strategic course is highly firm-specific, requiring a realistic analysis of a firm's current strengths, the changing needs and expectations of its client base, and a well-informed analysis of the options.

Regardless of whether you merge, join a network, create your own informal network, or collect a group of "best friends," be sure that you can continue to deliver the highest levels of local commercial and regulatory expertise to foreign clients and national ones. Small and midsize local firms that are successful at this sometimes describe themselves as "reliable guides" to the jurisdiction, or as offering "turnkey" services for clients investing in their countries. This is how, even when large, highly-capable, international firms enter a legal market, much of the best international legal work can continue to go to the best national and local law firms. ◆

# Refer a Friend to Join the ABA and the Section of International Law!

This is a fantastic opportunity to introduce your colleagues to a network of 17,000+ Section members worldwide. They can also join the Section's 50+ regional and practice specific committees FREE and enjoy many other Section benefits that will enhance their overall participation in ABA activities.

## Membership Benefits

- Global Networking via Committees, Communities, and City Chapters
- Professional Development & Education at the Fall Meeting in Miami, Florida, October 24–28 & at the Spring Meeting in New York, April 17–21, 2018
- Regional Forums in Asia, Europe and Mexico
- Leadership Appointments to Elevate Your Professional Profile
- Opportunities to Publish
- Career Advancement via Speaking Engagements at Section Meetings and Committee Programs
- International Projects to Advance the Rule of Law Around the World
- Nominate Someone or Yourself for Awards

To direct your friends and colleagues to join the ABA and the Section now, visit ambar.org/join and apply promotion code: DISCOUNTABA18 at checkout. As an Associate member the cost to join the ABA is approximately $80.00 and the Section is FREE! For Lawyer members, the rate will range from $50 to $250 depending on bar admission date.

**Visit ambar.org/join and use promotion code: DISCOUNTABA18**