FEDERAL BAR ASSOCIATION SOUTHERN DISTRICT OF NEW YORK CHAPTER

Spring 2016 NEW YORK MINUTES - The Newsletter of the Southern District of New York Chapter of the FBA

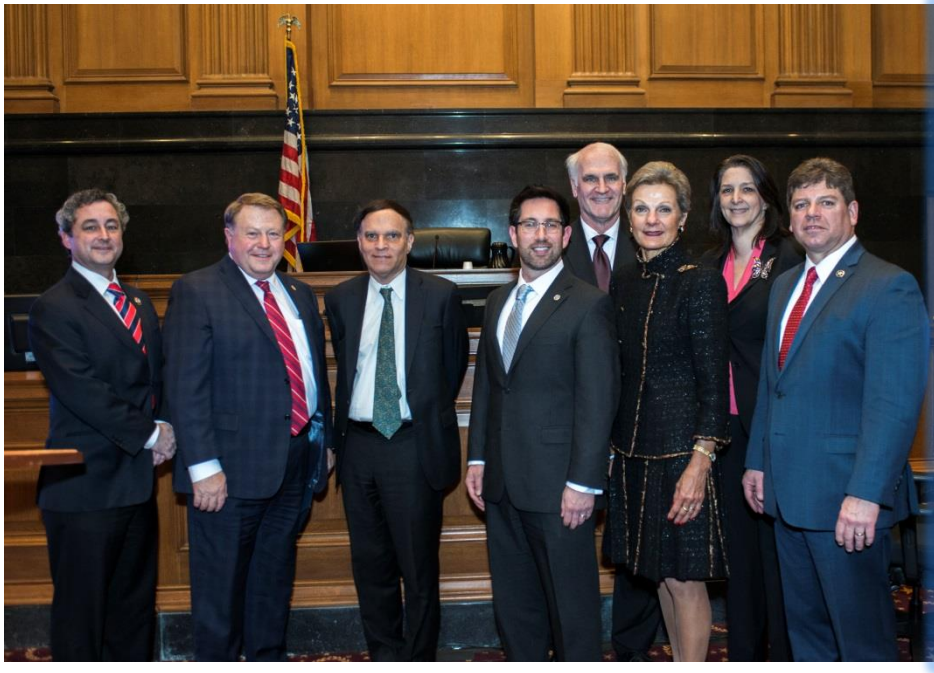
IN THIS EDITION

Newsletter Editors
Samuel Blaustein
Wendy Risa Stein

SDNY Chapter Events

Meet the SDNY U.S. Marshal, Michael Greco

February 23, 2016



(left to right)

Raymond J. Dowd, FBA National Director

Mark Vincent, FBA National President

Hon. Robert A. Katzmann
Chief Judge, Second Circuit

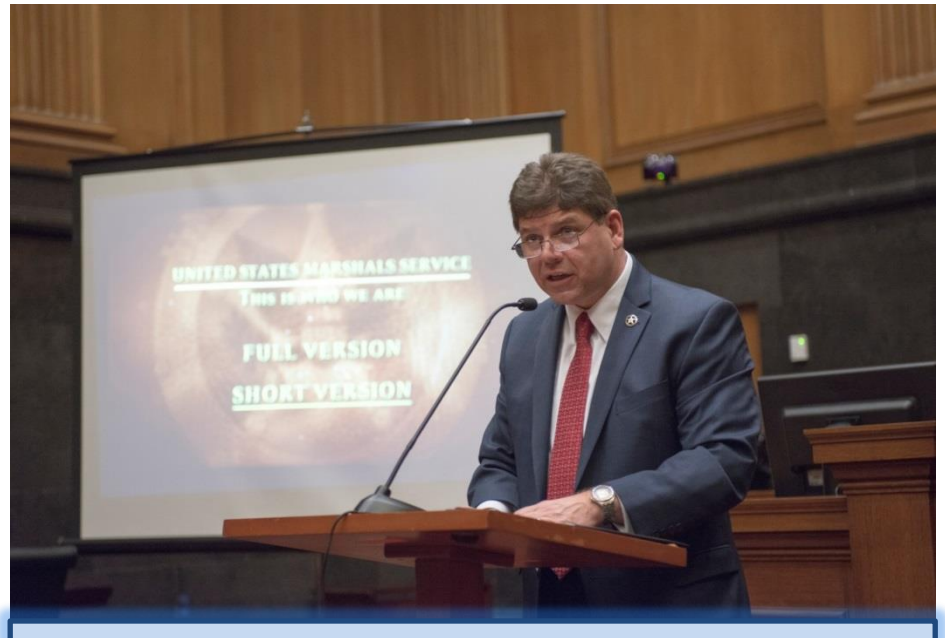
Michael J. Zussman
President, SDNY Chapter of the FBA

Hon. Timothy C. Stanceu
Chief Judge, Court of International Trade

Hon. Loretta A. Preska
Chief Judge, Southern District of NY

Karen Milton, Second Circuit Executive

U.S Marshal Michael Greco
Southern District of New York

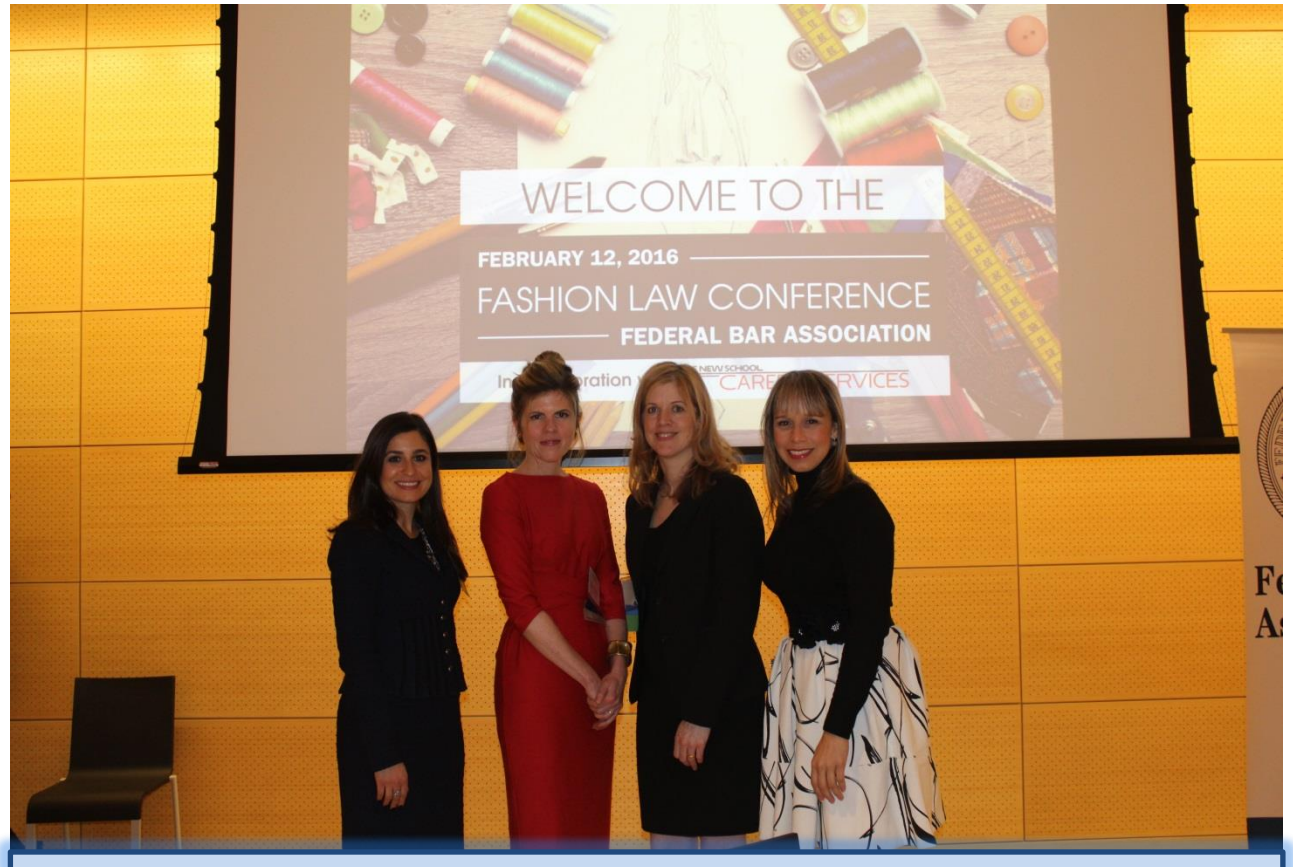


SDNY U.S. Marshal Michael Greco

SDNY Chapter Events

Fashion Law Conference

February 12, 2016



(left to right)
Maria Vathis
Olivera Medenica
Frances Hadfield
Katherine Gonzalez

Letter from the President

Dear SDNY FBA Members:

This Spring, the Southern District of New York Chapter continues to provide its membership with outstanding programs. On April 20, 2016, we celebrate the Hon. Loretta A. Preska, Chief U.S. District Judge, Southern District of New York, as Her Honor "passes the torch" as Chief Judge to the Hon. Colleen McMahon, U.S. District Judge, Southern District of New York. Chief Judge Preska has been a long time friend, supporter and active member of the Federal Bar Association, including as a member of the Federal Litigation Section board.

On February 23, 2016, our chapter hosted an event at the Thurgood Marshall Courthouse honoring U.S. Marshal Michael Greco, the Southern District of New York's first Latino Marshal. Marshal Greco gave a fascinating presentation on the many duties of the U.S. Marshals Service, with a video featuring John Walsh of America's Most Wanted, who is an honorary Deputy U.S. Marshal. Second Circuit Chief Judge Robert A. Katzmann and SDNY Chief Judge Preska gave opening remarks, and FBA National President Mark Vincent traveled to New York for this unique program.

On February 12, 2016, our chapter hosted the third annual Fashion Law Conference, a national FBA event focusing on IP and counterfeiting issues in fashion law, which featured top attorneys from Tiffany & Co., Estee Lauder and New York & Co., as well as top law firms.

Please contact Wendy Stein (wstein@gibbonslaw.com) if you would like to contribute an article to the New York Minutes: Please contact me at mzussman@cdas.com for more details about any of our upcoming events and to learn about how to become more involved with the Southern District of New York chapter. - Michael J. Zussman

JDGs: Not Always Equal, But Should Always Be Joint

Vicki Franks

In litigation, we sometimes find ourselves in the throes of cases with multiple defendants working as a Joint Defense Group or "JDG." Yet, in advocating for our client, we find ourselves at a fork in the road when joining such groups. What is our role here? Is there any group leader? How do we voice our opinions? Regardless of what questions you may face, as Yogi Berra once said, "when you get to the fork in the road, take it." That rings true here. If you find yourself joining a JDG, join it, be part of it, and enjoy it – whatever direction it takes you, it will provide an opportunity to not only work with attorneys outside your firm, but to share ideas and learn new tactics and styles while voicing your own. At the same time, it can also be an overwhelming situation of coordination and organization, pulling teeth for participation, and shifting sand beneath you from sporadic settlements along the way to trial. This article addresses, and provides pragmatic ideas, for how JDGs can maximize their expertise while maintaining a culture of a "joint" defense group.

I. What is a Joint Defense Group

A joint defense group stems from the idea that different, multiple parties represented by different attorneys may share a common interest, i.e., a common defense, in a litigation.[1]

What a joint defense group gains from a legal perspective is an exception to a potential waiver of the attorney-client privilege, namely, a joint-defense privilege. As the court in *HSH Nordbank AG v. Swerdlow*, explained, "Demonstrating the applicability of the common interest doctrine requires a two-part showing: '(1) the party who asserts the rule must share a common legal interest with the party with whom the information was shared and (2) the statements for which protection is sought [must have been] designed to further that interest.' . . . Such a showing often exists in those instances in which 'multiple persons are represented by the same attorney,' . . . or 'a joint defense effort or strategy has been decided upon and undertaken by the parties and their respective counsel.'"[2]

This article addresses how a joint defense group, once established, can operate to maximize its greatest asset: namely, a "brain trust."

II. Establishing Leadership

A leader is essential to the joint defense group—he or she can act as a central, organizing unit for cohesiveness amongst all members.

---

[1] See *Joint Defense Agreements: Balancing Risk and Reward*, Mark R. Robeck and Louis E. Layrisson III, ABA Energy Litigation (March 2011), available at http://apps.americanbar.org/litigation/committees/energy/articles/winterspring2011-joint-defense-agreement-risks.html.

[2] 259 F.R.D. 64, 71 (S.D.N.Y. 2009) (citations omitted).

Often a leader will emerge from a JDG naturally. It could be a partner at a "first-filer" law firm in a Hatch-Waxman litigation. Or it may be the partner at the firm that is ranked repeatedly by IP Law 360 as "Firms GCs fear the most." If a natural leader has not emerged, then the group may want to ask (i) who may be interested in leading the group and (ii) if there are multiple volunteers, a poll taken based upon vetting qualifications such as who has managed a litigation team and gone to trial before.

Nevertheless, what happens if a majority of the JDG does not like the way any group leader is running the case? Does majority group rule? While majority rule may seem like a good idea initially, JDGs are fluid groups. For example, members may come and go with settlements or the like, such that what is a "majority" one day may not be the "majority" the next.

Rather, discussing, professionally, any concerns a participant may have may better address how a case is proceeding. Additionally, if a participant is unhappy with the JDG leadership, raising only a disagreement or concern without providing an alternative or assistance to execute any proposed alternative may cause more harm than good. Constructive criticism and volunteering to assist in execution of any new plan goes much farther, and better deserves consideration by the group as a whole, than bantering and dismissing how any current leader is operating.

III. How Leaders Can Encourage Joint Participation

An effective leader can establish operating schedules that distribute work fairly and evenly, but maximize a group's particular strengths. For example, a guideline could be set—and enforced—that all firms be responsible for two fact depositions. If there is a key fact witness, drawing from the groups' expertise, that could be assigned to a particular member. A less important fact witness may be assigned to a young associate of a JDG member.

Additionally, timelines should be established for drafts. For example, draft deposition outlines could be circulated amongst all JDG members one week before any scheduled deposition for comment because a JDG is, or at least should be, "joint." For briefs or motions, a two-week deadline could be set.

How could a JDG leader enforce such rules? The leader could remind everyone that any party at any time may be in confidential settlement discussions and exit the JDG. The brief-writing responsibility would then necessarily shift to another member. If a draft brief is provided to the JDG two weeks before any non-extendable deadline, the group has a base document regardless if that party settles soon before the filing date. Otherwise, a party could intend to provide a draft to the JDG three or four days before a non-extendable filing date, settle before that third or fourth day, and leave the remainder of the JDG unnecessarily scrambling to write a brief in three days. Accordingly, a leader can explain that it is in the entire JDG's best interest to follow set deadlines for drafts.

Another reason that all JDG members should respect well-set draft deadlines is because attorneys are advocates for their individual clients (though in a group setting with some shared objectives). It could be that upon reviewing what will be the JDG's brief and argument, you want to submit your own brief. Having a two-week rule allows any one JDG member enough time to review and digest any brief, talk through any issues with the group as a whole, while at the same time preserving time if he or she needs to supplement that briefing with their own memorandum.

IV. How Leaders Can Utilize the Perks of a JDG

Remember that as an advocate for your client, you must take advantage of all resources available to you, and if that means giving nod to a member who repeatedly ranks as a top appellate attorney, hand over the reins. Or that firm may have a top trial lawyer who is renowned for opening statements. Again, hand over the reins. Despite the difficulties that may arise with a JDG, they present one unique feature: a brain trust. Egos must be set aside in favor of an objective analysis of who is most likely the best attorney for a certain task, based upon that attorney's qualifications, experience, and skill set. It may be that one client picks up a lion's share of the cost for a particular task, e.g., opening and closing statements at trial, but if there was no JDG to begin with, that client would be paying regardless. And the costs could be recouped by deferring another task to a separate member better suited for, e.g., arguing on appeal.

Additionally, if it is sometimes hard for a young associate to feel comfortable voicing opinions or concerns within his or her own firm, one can imagine how much harder it could be to do so amongst multitudes of seasoned attorneys from many prestigious firms. One way to address this, and ensure the brain trust is fully utilized (as young attorneys can provide insight too) is to form a 'break-out' group for them. For example, associates with 6 years experience or less could have a monthly conference call discussing case issues and projects. One leader of this associate group could then present ideas discussed by the associates collectively to the larger JDG group at a later time.

V. Always Remember You Are an Advocate for Your Client

Lastly, remember, "it ain't over till it's over," as Yogi Berra also said, and whether that be by trial or settlement, you must advocate for your client and remain actively engaged in and knowledgeable about the case throughout. A JDG may not always be equal because of the varying levels of expertise brought to the table by different members, but it must always remain joint. All attorneys have a core responsibility to remain active, interested, and knowledgeable about the JDG and the case.

Vicki Franks is Senior Counsel at the law firm of Frommer Lawrence & Haug, LLP. With 12 years of intellectual property experience—primarily in patent litigation—she routinely advises clients on strategies that are both successful in the courtroom and in the day-to-day marketplace. She has handled patent cases covering such technologies as wireless hand-held devices, veterinary recombinant vaccinations, pharmaceuticals subject to Hatch-Waxman litigation, textile and chemical engineering in the papermaking industry, and even the ergonomics of shower curtain hooks. She has written several peer-reviewed law review articles, including the lead article in the 2014 Federal Circuit Bar Journal, and enjoys presenting her thoughts at various speaking venues. Repeatedly ranked as a Rising Star in the NYC Metro Area Super Lawyers publication for patent litigation, Ms. Franks is committed to advancing client interests so as to achieve maximum value for their intellectual property rights. Additionally, she has successfully represented veterans through the pro bono efforts of her firm before the Court of Appeals for Veterans Claims, including obtaining benefits for a World War II veteran. More information about Ms. Franks, including representative cases and published pieces, can be found at http://www.flhlaw.com/franks/. She can be contacted at vfranks@flhlaw.com.

Cloud Computing: Privacy, Data Security and Contractual Considerations[1]

Wendy Callaghan and Heather Shea

Cloud models have become increasingly popular technology solutions for businesses across the globe. According to a May 2015 study published by the Economist Intelligence Unit and IBM, while one-third of companies say that 60% or more of their technology is cloud-based today, almost two-thirds believe this will be the case in two years' time.[2] Another recent study forecasts business spending of approximately $191 billion on cloud services by 2020, compared to $72 billion in 2014.[3] As companies rapidly adopt varied offerings of cloud providers, businesses continue to be responsible for safeguarding business data residing in the cloud, including the personal data of customers, employees and other individuals.

The purpose of this article is to provide an overview of the various cloud computing models available to organizations and to address at a high-level some important privacy, data security and contractual considerations when engaging a cloud provider.

What is Cloud Computing?

The National Institute of Standards and Technology ("NIST") defines "cloud computing" as:

> [A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Benefits of utilizing the cloud may include lower cost, reliability, resilience and improved security. A variety of cloud options exist, including three service models: (i) Infrastructure as a Service, wherein the cloud provider supplies storage, hardware, servers and networking components while the customer deploys applications; (ii) Platform as a Service, wherein the provider supplies operating systems and related services; and (iii) Software as a Service, wherein the provider delivers web-based applications hosted in a cloud infrastructure.

---

[1] The views expressed in this article are our own and do not necessarily represent the views or positions of American International Group, Inc.

[2] Mapping the Cloud Maturity Curve, http://public.dhe.ibm.com/common/ssi/ecm/ku/en/kul12355usen/KUL12355USEN.PDF at 7.

[3] *See* 2015 Top Markets Report Cloud Computing: A Market Assessment Tool for U.S. Exporters, Department of Commerce International Trade Administration, July 2015, http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf at 3-4.

There are also several cloud deployment models. For example, a "public cloud" is one shared by multiple consumers and owned and controlled by the cloud provider. In contrast, a "private cloud" is one dedicated for exclusive use by a single organization, which may be located on the organization's premises or elsewhere. Yet a third option is a "community cloud," one shared by organizations with common requirements. A "hybrid cloud" is a combination of private and public clouds, with orchestration to direct in which environment workloads will reside. Organizations may opt for a hybrid model to leverage the private cloud component for certain data and applications, while utilizing another cloud environment for other data and applications.

Privacy and Data Security: Legal/Regulatory Landscape

Before contracting with a cloud provider, businesses will likely want to consider the types of data and sensitivity levels associated with data that the business aims to migrate, which privacy and data security laws, regulations or industry standards may be implicated by such migration, and whether the cloud offers appropriate security to safeguard the information at hand.

The U.S. privacy and data security landscape contains varied requirements ranging from federal and state-level sector-specific laws and regulations governing sensitive categories of information like financial data (*e.g.,* the Gramm-Leach-Bliley Act ("GLBA") regulating use and disclosure of "nonpublic personal information" by financial institutions) and healthcare information (*e.g.,* the Health Insurance Portability and Accountability Act ("HIPAA")), to general consumer protection laws (*e.g.,* Section 5 of the Federal Trade Commission ("FTC") Act, empowering the FTC to prevent "unfair or deceptive acts or practices in or affecting commerce,"[4] and state consumer protection laws). A number of other relevant state laws also exist, including 47 different state data breach notification laws. These laws generally require notification to affected individuals – and sometimes regulators, law enforcement, or others – when certain unencrypted, computerized personal information, like Social Security numbers or financial account information, is accessed or acquired without authorization. Finally, industry standards like the Payment Card Industry Data Security Standard, which specifies data security obligations for those that process, store and transmit payment card information, are also relevant.

Certain of these assorted laws, regulations and industry standards address a business's obligations with respect to service providers, including cloud providers, or apply directly to third parties. For instance, the GLBA Safeguards Rule mandates that financial institutions "oversee service providers," by "(1) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) requiring . . . service providers by contract to implement and maintain such safeguards."[5] In

---

[4] https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf.

[5] 16 C.F.R. § 314, codifying the FTC Safeguards Rule.

addition, HIPAA renders cloud providers operating as "business associates" directly liable for non-compliance with the HIPAA Security Rule and certain components of the HIPAA Privacy Rule.[6] HIPAA further requires covered entities to execute business associate agreements to ensure proper use, disclosure and safeguarding of protected health information.

Moreover, recent FTC enforcement actions should be monitored. A business's general failure to perform adequate due diligence, incorporate contractual requirements to safeguard personal information or oversee a cloud provider's security could be deemed an unfair or deceptive trade practice. In January 2014, GMR Transcription Services, Inc. ("GMR") settled an FTC enforcement proceeding resulting from the unauthorized internet disclosure of patients' sensitive medical information due to the inadequate security practices of GMR's audio transcription contractor, Fedtrans. The FTC alleged that GMR and its owners violated Section 5(a) of the FTC Act by, *inter alia*, failing to: (1) contractually require Fedtrans to implement reasonable and appropriate security measures to protect personal information, and (2) monitor whether Fedtrans actually employed adequate security measures to protect personal information.[7]

Non-U.S. data protection laws and regulations should also be considered, where applicable. In Europe for instance, the current E.U. Data Protection Directive 95/46/EC and national laws of 28 E.U. member states will soon be replaced by the recently agreed-upon General Data Protection Regulation (the "Regulation"), expected to be effective Spring 2018. Noteworthy features of the Regulation include extraterritorial applicability to businesses outside of Europe that process personal data of Europeans, significant fines and penalties (up to 4% of global turnover) for non-compliance, and new data breach notification guidelines requiring notification to a supervisory authority ". . . without undue delay and, where feasible, not later than 72 hours after having become aware of it . . . unless the controller is able to demonstrate . . . that the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals."[8]

Cloud service engagements contemplating the cross-border transfer of personal data may also need to comply with international data transfer, data localization or data residency laws that restrict the movement of data outside of country borders. In October 2015, cross-border data transfers garnered increased attention when the European Court of Justice in *Schrems v. Data Protection Commissioner* (Case C-362/14) invalidated the fifteen year-old E.U.-U.S. Safe

---

[6] *See* HIPAA Final Omnibus Rule, effective March 26, 2013, https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf at 5589, 5591-5592.

[7] *See In Re GMR Transcription Services, Inc.*, Docket No. C-4482, Complaint, August 14, 2014, https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter.

[8] Regulation (EU) No XXX/2016 of the European Parliament and of the Council, Art. 31, http://static.ow.ly/docs/Regulation_consolidated_text_EN_47uW.pdf.

Harbor framework relied upon by many companies, including cloud providers, to lawfully transfer personal data from Europe to the U.S.[9] This sea change in the law required companies to begin relying on alternative, lawful mechanisms to transfer data from Europe to the U.S. In February 2016 American and European officials negotiated a replacement data transfer agreement, the "E.U.-U.S. Privacy Shield," which is currently pending final adoption by the E.U. The implications of the *Schrems* decision on this pact and other data transfer mechanisms remain to be seen.

These and other international legal considerations, as well as cloud-specific guidance published by regulators, influence corporate decisions about what data to migrate to the cloud, which cloud solutions are appropriate and what contractual terms the parties should enter into.

Contracting with a Cloud Provider: Common Provisions in Cloud Contracts

Although not an exhaustive list, below are common components of cloud contracts related to privacy and data security.

1. Permissible use and sharing of customer data

The scope of what cloud providers can and cannot do with customer data often plays a prominent role in cloud contracts. For example, contracts may address whether providers may share customer data with sub-contractors or use customer data for their own purposes. Where cross-border data transfer or data localization requirements apply, contracts often address the mechanisms for transfer and identify the geographic locations where customer data will reside.

The contract may also specify how providers should respond to a third party subpoena or warrant seeking data access. A case currently pending before the Second Circuit, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.* 13 Mag. 2814 (S.D.N.Y. Apr. 25, 2014)), concerns Microsoft's refusal to turn over a customer's emails stored in Ireland in response to a U.S. law enforcement warrant.

2. Security

Specific security requirements (such as when encryption is required), including obligations mandated by applicable law, are commonly incorporated into cloud contracts. Contracts may also address which parties (customer, regulator or independent third party) can audit compliance

[9] *See Schrems v. Data Protection Commissioner* (Case C-362/14), http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d50b096b3d36ba4ebb895adb6b7fddc095.e34KaxiLc3qMb40Rch0SaxuSbx90?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1309160 (invalidating Safe Harbor and finding that transfers to the U.S. violate fundamental principles of European data protection law based largely on U.S. government access to data and the lack of European citizens' right to judicial redress in U.S. courts).

or conduct a data center inspection, the frequency of such audits, and whether ongoing monitoring will be permitted and by whom.

3. Losses, Claims, Costs and other Remedies

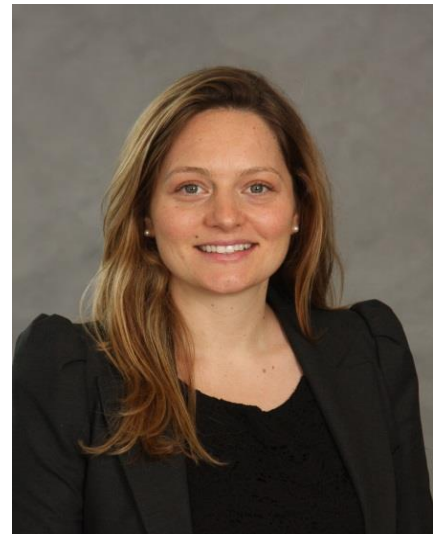
Contracts may also specify who will pay the costs and expenses associated with loss of, damage to or compromise of customer data, including breaches of security, confidentiality and integrity of personal information. Indemnity provisions may address coverage for associated third party claims, while the parties may allocate responsibility for costs to remediate a data breach (*i.e.*, costs to investigate the cause of the breach, mail breach notification letters, pay for credit monitoring or identity theft protection services, or pay regulatory fines and penalties). In addition, termination rights may be triggered by a data breach, including those circumstances where the breach can be tied to the provider's failure to meet contractual obligations.

The Future

As cloud services, privacy laws and data security standards continue to evolve, the ways in which businesses, cloud providers and regulators approach cloud computing arrangements are also likely to change. Parties negotiating cloud agreements should be mindful of this evolving landscape when initiating an engagement and should continue to monitor developments once the relationship is underway.

Wendy Callaghan is Associate General Counsel and Head of Emerging Technologies and Digital in the IT Law Department of American International Group, Inc. (AIG). Wendy advises domestic and international AIG member companies on IT legal issues. She has extensive experience negotiating complex technology transactions, including cloud deals.

Prior to joining AIG, Wendy was a member of the Technology Practice Group at Pillsbury Winthrop Shaw Pittman, LLP (formerly Shaw Pittman, LLP). She is a graduate of Rutgers School of Law, where she graduated with High Honors, and the State University of New York College at Oneonta, where she graduated *Summa Cum Laude*. She is licensed to practice law in New York and New Jersey.



Heather Shea is an Associate General Counsel and Senior Compliance Officer in the Global Compliance Group of American International Group, Inc. (AIG). Heather assists with the management of AIG's global privacy and records management compliance programs. She regularly advises AIG and its businesses on privacy, data security, records management and information governance matters. Heather serves on AIG's Pro Bono Committee and is actively involved in pro bono work.

Prior to joining AIG, Heather was an associate in the Litigation Department of Weil, Gotshal & Manges, LLP. Heather is a graduate of Georgetown University, the London School of Economics and Political Science, and Fordham University School of Law. She is a Certified Information Privacy Professional (CIPP/US) and is licensed to practice law in New York and Massachusetts.

Mark Your Calendar!

April 13, 2016: Meet the White Plains SDNY Judges
Please join us in White Plains, NY to meet the White Plains District Judges.

April 20, 2016: Passing the Torch
Please join our chapter in a "Passing the Torch," program, as we honor and celebrate outgoing SDNY Chief Judge Loretta A. Preska and incoming SDNY Chief Judge Colleen McMahon.

May 6, 2016: Admiralty and Maritime Law Event
In connection with the Maritime Lawyers Association annual meeting, our chapter's new Admiralty and Maritime Committee will co-sponsor a brown bag lunch at the Second Circuit to discuss issues in maritime and admiralty law with the Hon. John G. Koeltl, U.S. District Judge, SDNY.

May 17, 2016: Advanced Health Care Directives at the Federal Court
Our chapter's new Health Law Committee is hosting its first event as part of the FBA's National Community Outreach Program and National Health Care Decisions Day: Advanced Health Care Directives, a workshop to help federal court staff with end of life planning, such as living wills and health care proxies.

May 19, 2016: Capitol Hill Day
Please consider participating in this important event as FBA leaders from across the country meet with House and Senate offices to discuss important FBA legislative issues that impact the administration of justice and the federal courts. Participants will be provided guidance in scheduling meetings with lawmakers and briefed on the legislative issues leading up to Capitol Hill Day.

June 8, 2016: Venture Law Financing
Hear the story of one founder's journey from incorporation, through a series of financing rounds, to an equity purchase by a public company. She will be joined by one of her VC investors and attorneys.

WWBA

WESTCHESTER WOMEN'S BAR ASSOCIATION

Federal Bar Association

Southern District of New York Chapter

WHITE PLAINS Bar Association

WWBA General Membership Meeting

Co-Sponsored by the Federal Bar Association, S.D.N.Y. Chapter &
the White Plains Bar Association

"A Conversation with U.S. District Judges Hon. Cathy Seibel & Hon. Vincent L. Briccetti"

Join us as Judges Seibel and Briccetti share best practices and "do's" and "don'ts" for practice in the S.D.N.Y. in White Plains

Moderators:
Hon. Lisa Margaret Smith
Donna Frosco, Esq.

Date:	Wednesday, April 13, 2016
Time:	5:30 p.m. registration and light dinner, 6:00-8:00pm program
Place:	La Bocca Ristorante 8 Church Street White Plains, NY 10601 (914) 948-3281
Charge:	$60.00 WWBA, FBA and WPBA members $70.00 non-members (Checks payable to "WWBA")
RSVP:	**By April 8, 2016** on-line at www.wwbany.org or via e-mail at executivedirector@wwbany.org

Attendance is strictly limited to WWBA, FBA and WPBA members and their invited guests.

The opinions expressed by any program presenter are the presenter's own, and do not reflect the official position of the WWB, FBA or WPBA

Federal Bar Association

Southern District of New York Chapter

Please join

The Federal Bar Association

in congratulating

Chief Judge Loretta A. Preska

On Her Tenure as Chief Judge

and to congratulate

Judge Colleen McMahon

Who Will Succeed Her as Chief

April 20, 2016

5:30–7:30pm

Thurgood Marshall Courthouse
Main Floor

Please RSVP to dlesser@morrisoncohen.com