BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

November 2012

Feature Articles

BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

Our Mini-Theme: Developments in Cyberspace

The Cyberspace Law Committee (CLC) is gearing up for its annual stand-alone meeting: The CLC 2013 Institute on the Law of Cyberspace and Winter Working Meeting will take place January 25–26 at the W Los Angeles-Westwood Hotel. With this mini-theme, we offer three articles on changes in longstanding regulatory regimes governing business in cyberspace alongside analyses of newly-emerging cyberlaw topics, which we will explore further at the January conference as part of a broader cyberlaw agenda. First in our mini-theme, law professor Gregory Voss of the University of Toulouse in France provides a valuable update on the proposed new European Union General Data Protection Regulation, which seeks to create more uniformity in data protection laws across Europe. The new regulation would also expand the definition of "personal data" at issue in many of its provisions. It would create new data breach reporting requirements in member countries and address the growing concerns about data portability and the so-called "right to be forgotten." Professor Voss offers some insight into the process behind the potential implementation of this new regulation along with some useful summaries of the new requirements and suggestions for non-EU lawyers counseling businesses mindful of the evolving regulatory framework.

Second, John Pavlolotsky of San Francisco offers a timely introduction to a rapidly evolving area of online business where the applicability of existing privacy, data security, and other laws and regulations has barely begun to play out: "Big Data" analytics. Moving quickly from a slightly esoteric engineering concept to a widely-used Silicon Valley buzzword, the phrase "Big Data" has come to be understood as the problematic area of large data sets, where the velocity, veracity, and variety of the virtual (online) data is so enormous that conventional methods of analysis are impractical. John offers a summary explanation of the concept and how it has been addressed or discussed by courts and by the law, if at all, so far.

Finally, with a discussion of the still quite unsettled application of existing principles of law to a developing area of concern about the backbone of the Internet, cyberlawer Ernesto Rubi of Miami offers an analysis of the potential legal treatement of rights in IPv4 numbers, the globally unique identifiers that are linked to every device or home page (laptop, smart phone, desktop, website, tablet, etc.) that accesses the Internet. Rubi discusses potential ownership rights in of IPv4 numbers, despite the purported restrictions on transferability of IPv4 numbers imposed by the registries involved with IP assignment. Given the finite set of global IPv4 numbers for assignment, the continued massive growth in Internet-enabled devices and global demand for access, along with the slow evolution of the next systems of Internet identification assignment, this is an area that certainly will attract more attention soon.

Join us in Los Angeles in January for a high-powered two-day conference that will delve deeper into a host of cyberlaw topics such as these along with presentations on cybersecurity and the cloud, issues raised by new models of digital content distribution, the continuing problems with consumer online contracting, and the most significant cyberlaw cases of 2012. We will also roll up our sleeves and jump into interactive roundtables on a variety of cyberlaw topics, and will devote the second part of the conference to break-out sessions on many of the writing and presentation projects of the Committee's subcommittees and task forces. All these are open sessions and provide a terrific opportunity to those new to the Committee, the Section, or the ABA to get involved in some of the most significant and most current topics of the day involving the applicability of the rule of law to the ever-changing world of business and technology.

Jonathan T. Rubens
Chair, Cyberspace Law Committee

Additional Resources

For related products and materials from the Cyberspace Law Committee, please see the following:

Internet Law for the Business Lawyer, Second Edition

BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

Preparing for the Proposed EU General Data Protection Regulation: With or without Amendments

By W. Gregory Voss

Viviane Reding, the European Commission vice-president and justice commissioner, launched a proposal on January 25, 2012, for a new EU Data Protection Regulation, referred to as the "General Data Protection Regulation" (GDPR). If adopted, the GDPR would reshape the European data protection framework in a harmonious way, ensuring EU residents a high level of protection for their personal data. Already, this European Commission proposal has elicited much attention in the legal and business world. After putting the GDPR in perspective, this article will: Briefly discuss legislative action and the time frame, set out some important (and sometimes controversial) provisions, and attempt to draw lessons for businesses.

The GDPR in Perspective

The proposed GDPR arises in a context where the protection of personal data in a constantly (and rapidly) evolving technological context is a concern on both sides of the Atlantic. One manifestation of this concern is the High Level Conference on Privacy and Protection of Personal Data held simultaneously in Washington and Brussels, which led to a joint statement on March 19, 2012, by Viviane Reding and former U.S. Secretary of Commerce John Bryson, emphasizing the need for more interoperability of European and U.S. privacy systems "on a high level of protection."

A Need for Greater Uniformity in EU Law

The choice of a regulation as the EU legislative instrument to achieve such a high level of protection was made because regulations become law in the same form in all of the current 27 Member States of the EU and in new Member States, thereby promoting uniformity of law in the EU, which contrasts with the differing ways in which the current Data Protection Directive (Council Directive 95/46) (the "Directive"), which was adopted in 1995, was subsequently implemented (or "transposed") by national law in the various EU Member States. This divergence in implementation occurred in spite of compliance with the required minimum standards of the Directive.

Such divergence was made possible because, according to Article 288 of the Treaty on the Functioning of the European Union, as in force today, it is left up to the "national authorities" of the Member States to choose the "form and methods" of the implementation of directives. For example, France may act to implement a directive by the method of adoption of a bill in the French parliament or by a presidential decree, when the French president is so empowered. Likewise, Spain, within some limits, may choose a different form for the instrument by which it implements a directive than that chosen by France, so long as the result to be achieved is so achieved.

Now, multiply this situation by each of the 27 Member States to which the directive is addressed, and you can see how a possible result is divergence.

The Potential Positive Effects of Increased Trust

One of the objectives of the European Commission in proposing the GDPR is to increase trust in the use of information services by EU users, while protecting their fundamental rights. It is thought that increased trust should encourage a further development of information services in the EU, furthering its digital agenda and providing economic advantages to companies, such as increased sales, and to the European economy, through additional growth and greater employment. Neelie Kroes, EU digital agenda commissioner, recently highlighted the importance of trust (or lack of distrust) in the establishment of "new and bigger markets."

New Technology Leads to New Challenges to Privacy

The area of data protection is one in which Europe has much experience both at the Member State level (for example, France had a statute as early as 1978), and at the EU level (the Directive, followed by over 10 years of application). One may also highlight in passing the difference in the European "global" approach to privacy and personal data protection and the U.S. "piecemeal" approach, with legislation crafted for specific sectors or issues. Nonetheless, because of the technological advances realized in the ensuing years and unforeseen in 1995, such as biometrics, facial recognition software, increased data storage capacities, cloud computing systems, and social networks, more personal data (and more intimate personal data, in all senses of the term) are collected and processed. This has resulted in new challenges to privacy, which has led the European Commission to propose the replacement of the Directive with a new data protection framework, including the GDPR.

Legislative Action and the Time Frame

Although today it is uncertain whether or not the GDPR will be adopted and, if adopted within which time frame, we already have some indications as to the preliminary legislative action and certain elements of the potential time frame. For example, a tentative calendar for the GDPR published in May 2012 by its rapporteur in the European Parliament foresees the GDPR coming to a vote before that legislative body in early 2014.

The European Parliament

The LIBE (Civil Liberties, Justice and Home Affairs) Committee of the European Parliament has been appointed as the main committee with responsibility for the GDPR, although other committees are involved, i.e., Internal Market and Consumer Protection (IMCO), Industry, Research and Energy (ITRE), Economic and Monetary Affairs (ECON), Legal Affairs(JURI), and Employment and Social Affairs (EMPL), possibly indicating that the parliament considers the fundamental rights elements of the GDPR of greater importance than the economic ones, while acknowledging that economic elements are present. Recently, a meeting on the proposed data protection reform was organized with members of national parliaments, and the LIBE Committee should also be presenting a draft report on the data protection reform by the end of 2012.

The Council of the European Union

However, the European Parliament and the European Commission are not the only EU institutions involved in the data protection reform process. The Council of the European Union (EU Council), through its working parties, is also reviewing the proposed GDPR and is discussing amendments to it. The EU Council's Working Party on Data Protection and Exchange of Information (DAPIX) has suggested proposed changes to certain articles of the GDPR. In addition, there are divergent views in various Member States on several provisions of the GDPR, and even as to the choice of a regulation as the appropriate legislative instrument. One element of the GDPR that has also been criticized is the Commission's role to act through delegated and implementing acts (for example, enabling of the Commission to adopt delegated acts to specify criteria and conditions and for processing special categories of personal data), as this might be considered to give the Commission too much discretion in defining the application of the GDPR.

Council/Parliament Interface and Entry into Force

Earlier this year, a EU Council spokesman indicated that negotiations between the EU Council and the European Parliament on the text of the GDPR should begin at the end of 2012. Agreement between those two institutions on the text of the GDPR in two successive readings is required for it to become binding and directly applicable in Member States. The GDPR's entry into force would occur 20 days after publication in the Official Journal of the European Union, however in the current proposal, it would only apply two years after such date (this time frame, however, is indicated between brackets and in italics, suggesting that it is a point open for discussion). To be clear, with the information available today, the start of the application of the GDPR (if adopted) should be expected to occur sometime during the period of 2014–2016, absent unforeseen blockages such as those which occurred during the adoption of a famous recent EU regulation in another field – REACH (chemicals and the environment).

Some Important Provisions of the GDPR

Effect on Non-EU Companies

In its current form, the GDPR would apply to controllers of personal data not established in the EU, so long as they process EU residents' personal data related to the offer of goods or services in the EU or to behavioral monitoring. (A "controller" would include a company that collects and processes its customers' information; for example, a company that has a customer relationship management program.)

Viviane Reding has been firm on this point, but it remains to be seen whether future EU–U.S. discussions will cover this issue under the GDPR, as was done under the Directive when the 2000 Safe Harbor for transatlantic data transfers was negotiated. (It should be noted that the GDPR also contains provisions on cross-border data flows.)

Greater Uniformity of EU Law

Through its unifying effect on EU data protection law, the proposed GDPR would allow businesses operating in various EU Member States greater visibility and legal certainty in the field. (However, the delegated authority discretion of the

European Commission has the opposite effect.) In addition, the proposal for the GDPR provides that where a personal data controller or processor is established in two or more Member States, the EU Member State data protection authority of the place where the controller or processor has its main establishment would be able to supervise the activities of the controller or processor in all Member States. For example, if a company that controls or processes EU residents' personal data has its main European establishment in Ireland, it would be able to be supervised by the Irish data protection authority, and complete EU administrative filings and formalities there for all of the EU Member States in which it operates. This is the GDPR's "one-stop shop" provision that is designed to ease administrative formalities for some businesses, saving them time and money. Furthermore, a mechanism to ensure consistency in the application of the GDPR throughout the EU would be established.

On October 5, 2012, the Article 29 Working Party (WP29) – an independent advisory panel providing interpretative guidance on privacy directives to Member States – issued a second opinion on the data protection reform discussions and highlighted areas for "further debate and clarification" identified by the LIBE Committee of the European Parliament such as, among others, the attribution of roles in cross border cases between the various data protection supervisory authorities.

Delegated and Implementing Acts

WP29 included on the LIBE list of areas for additional work the role of the Commission to act through adopting "delegated and implementing acts." As the WP29 opinion makes clear, these delegated and implementing acts have been made possible by the Lisbon Treaty and are based on, respectively, Article 290 and Article 291 of the Treaty on the Functioning of the European Union. Delegated acts may be used to supplement or amend the GDPR for non-essential elements. Implementing acts may be used to ensure uniform implementation of acts throughout the EU. The EU Council and the Parliament have a two-month period during which they may object and block entry into force of delegated acts.

WP29 is concerned that enabling the European Commission in the GDPR to adopt delegated and implementing acts from the start (and broadly, as this possibility is offered in many articles of the proposed legislation), without the need for making a determination of their necessity on a case-by-case basis, there is a lack of legal certainty, with the Commission being given broad discretion, which in many cases, could be handled alternatively (e.g., by interpretative guidance, through national law, or detailed in the GDPR itself).

Broad Definition of "Personal Data"

By contrast, WP29 defends the GDPR against criticism of its broad definition of "personal data," as this is considered necessary in order to "future-proof" the proposed regulation in the context of rapid technological change. Under the GDPR, any information related to a natural person who can be identified by ways likely to be used by the controller would be caught under the definition.

By contrast, in Article 2(a) of the Directive, "personal data" is defined with respect to a person who is or can be directly or indirectly identified, particularly by "reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Thus, the GDPR allows for the possibility of technological advances leading a controller to identify an individual through other sorts of data, which would then be protected as "personal data" under the GDPR.

Data Breach Notification

Nonetheless, there are some additional requirements with which businesses subject to the GDPR will have to comply if the GDPR is adopted in its current form. To start, data controllers or processors will be required to report data breaches to the relevant data protection agency "without undue delay," and where feasible, within 24 hours of notice of such a breach. Notifications after such time period will need to be justified. Processors must inform controllers of breaches immediately after their establishment, and the controller must inform the data subject "without undue delay" if the breach will likely have a negative effect on the protection of the subject's personal data or privacy, unless the controller can prove that the data was rendered "unintelligible" to unauthorized persons.

Data Protection Impact Assessments

Data processing that presents "specific risks," such as that which involves certain sensitive information (e.g., health, race, ethnic origins, sex life, etc.), triggers the GDPR requirement for a data protection impact assessment. This assessment, which must describe the processing foreseen, shall assess risks to data subject rights and freedoms, means of addressing these and those designed to protect personal data, and demonstrate compliance with the GDPR. The views of data subjects on the processing must also be sought. The data protection impact assessment is to be accomplished by or on behalf of the controller (thus, at its expense), and the Commission may adopt further criteria by delegated acts.

Data Protection Officers

Where data are processed by enterprises with more than 250 employees, under the proposed GDPR the controller and the processor must appoint a data protection officer (DPO) who has expert knowledge on data protection law. This DPO may be an employee or an independent service contractor. Concern has been expressed that this may create a great administrative burden on the smaller of these companies, which could be described as SMEs, and that other factors, such as the degree of risk related to the processing activity, should be considered before placing ad-

ministrative burdens on such companies, instead of basing this requirement on the number of employees in the enterprise.

Data Portability and the Right to Be Forgotten

Two new rights introduced in the GDPR are data portability and a general right to be forgotten. In the first of these two, data controllers must provide a data subject's data to him or her in a format that allows transmittal into another data processing system, making them "portable." In the second, a data subject may require that all of his or her data be erased under certain circumstances, such as when he or she decides to revoke consent to processing.

Increased Fines

Fines for data protection violations by one of the most famous targets of data protection authorities in Europe – Google, for its Street View service – ranged from €100,000 to €1,000,000 in certain EU jurisdictions in 2011. If the GDPR is adopted in its current form, fines for data protection violations could rise significantly, as the proposed legislation provides for a sliding scale of fines, depending on the seriousness of the offense, whether it is a repeat offense and intentional, and whether the violator is an enterprise or not. For an enterprise, sanctions may involve a simple warning for a first non-intentional offense by an enterprise of less than 250 employees only engaging in processing as an ancillary activity, to a maximum of 2 percent of annual worldwide turnover for certain serious acts committed intentionally or negligently, with intermediate steps on the scale of 0.5 percent and 1 percent of annual worldwide turnover for violations of an intermediate seriousness. For certain large companies this could result in fines of hundreds of millions of euros or more.

Many other interesting provisions are included in the GDPR, such as privacy certifications, the possibility of appointing a representative in the EU for a non-EU company, and so on – too many for this short article, which is a nice transition to our lessons, including the first one on getting to know the GDPR.

Lessons for Businesses

Going forward, we may expect that there will be amendments made to the GDPR. Nevertheless, the European Commission has the drafter's advantage in that the other European institutions are working off the language of its proposal. In addition, there seems to be broad agreement as to the need for a revised data protection framework and greater harmonization of EU law in the area. From the GDPR and from related WP29 guidance, there are lessons to be drawn for businesses, in order both to reduce the risk of GDPR sanctions, on the one hand, and to increase trust and improve reputation, on the other. What follows is an attempt to elucidate some of these lessons.

1. *Put the GDPR on Your Radar*
   Become familiar with the GDPR and follow its development. Whether or not the provisions of the GDPR are adopted in their current form, many of the issues covered will not go away. Reform is needed. Becoming familiar with the issues now, and following the genesis of the future regulation will allow companies better to prepare for the final legislation. Legal monitoring may be considered part of good corporate legal strategy and even a necessity in today's competitive business world, and for the international firm, EU data protection legislation is no exception to the rule.

2. *Audit Risks for Potential Data Protection Violations*
   Companies should try to identify areas where potential data protection violations may occur, through auditing risk areas (for example, procedures for handling consent) – and may consider having this done by outside specialists. The results of these audits will allow them to identify and take measures to prevent such violations from happening. This certainly involves compliance programs.

3. *Incorporate Data Protection into Compliance Programs*
   Another lesson to be learned is to be proactive and, if has not already been achieved, incorporate data protection into compliance programs. The potential risks for non-compliance under the terms of the proposed GDPR are great in terms of potential financial risks, but also in terms of loss of customer trust and harm to reputation. Preventing these risks through adopting adequate procedures and increasing internal knowledge through training (seminars and other means meant to raise awareness) are crucial. Follow-up of compliance efforts should be performed. This method of being proactive may make a company more competitive than its counterparts who "put out fires" instead.

4. *Make Sure Proper Consent is Obtained*
   Where consent is required, it should be explicit, verifiable, and informed, and it should be obtained from data subjects prior to processing their personal data. The proposed GDPR places the burden of proof for this on the controller. Privacy policies should be reviewed in this light. Adequate procedures allowing for the data subject to revoke their consent should also be provided for.

5. *Incorporate Privacy by Design*
   An additional way of being proactive is by building privacy into the technology and organization and by ensuring a high level of data security by design. Companies may reduce potential risks related to data security breaches and privacy violations in this way.

6. *Prepare for Data Breaches*
   No one wants a data breach; however, with new rules as to notification of data breaches, developing the means of identifying them, and communicating about them rapidly – including between the controller and the

processor – may make the difference in reducing the harm created by such breaches and in helping to comply with the GDPR.

Many of these lessons are mere common sense. Some of them require some time to implement, so the earlier the better, in the perspective of a potential application of the GDPR. Whether or not the GDPR is adopted, following the above lessons now should help companies best prepare themselves in the eventuality that the GDPR is adopted – either in its current version, or with amendments.

W. Gregory Voss is a professor of business law economics at Toulouse Business School, Toulouse University, and member of the Institut de Recherche en Droit Européen International et Comparé (IRDEIC), Toulouse, France.

BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

Demystifying Big Data

By John Pavolotsky

Much has been written in business journals and blogs about "Big Data," which refers to the recent proliferation in data volumes and types that are so large, diverse, and unstructured it is difficult for current technologies to store and analyze. In short, the rapid innovation and deployment of technologies that capture data – from GPS-enabled smartphones and tablets, to RFID tags, to the millions of cameras used by business and consumers to record daily activities – has outpaced the development of technologies to store, organize, and analyze the massive data sets.

The *Harvard Business Review* devoted its October 2012 issue to the subject of Big Data, with articles titled "Big Data: The Management Revolution," "Making Advanced Analytics Work for You," and "Data Scientist: The Sexiest Job of the 21st Century." Many articles address various technologies designed to help manage Big Data, and others discuss the advantages Big Data can bring to a company's marketing efforts or warn of the dangers of Big Data to individual privacy. At least one recent article, "The Death of Big Data," published on October 4, 2012, on Forbes.com, argues that "Big Data" will soon become "Any Data," because massive data volumes, comprised predominantly of unstructured data, are quickly becoming the norm. While business publications have written widely about Big Data, legal commentators have written sparingly on the subject. This article will explore the unique and not-so-unique legal issues that it raises.

The Business of Big Data

The tools and business applications of Big Data are varied and many. Developers are increasingly offering software applications that ingest, organize, and store data streams, such as social media feeds. To help cope with this massive collection of data, other technology vendors are focused on data integration, which becomes extremely important if your data is stored on a variety of unconnected devices in different formats, or analytical tools to help extract useful business information form the collected data. Collectively, these technology companies are trying to advance algorithms to harness the massive collected data to assist in better product development, power targeted advertising, devise more effective marketing campaigns, power e-commerce recommendation engines, assist dynamic pricing, or improve any number of other business functions.

Notably, in the world of Big Data, there is a fundamental divide. On the one hand, some companies have for years been collecting, analyzing, managing, and storing tremendous amounts of data. These include certain e-commerce concerns and online search engines. In "Big Data: The Management Revolution," Andrew McAfee and Erik Brynjolfsson astutely point out: "Online businesses have always known that they were competing on how well they understood their data." Similarly, as early as the mid-1990s certain brick-and-mortar retailers were building massive data warehouses populated by transaction and other data. This first group can be called "data mavens." Others are new(er) to Big Data and thus face steeper learning and adoption curves. This second group can be called "data tyros."

Both groups must address a number of business questions. First, as a practical matter, is there actually meaning in the data? As a corollary, are there enough people (data scientists) qualified or capable to make sense of such data? Massive amounts of data are being collected and stored (because it is now cheap to do so), but whether or not most of that data has any value remains to be seen.

The Legal Landscape: Case Law

As noted, few have written about the legal implications of Big Data, and of those, most have focused on privacy issues. It could be that Big Data issues are just data issues, or Internet issues, or device (e.g., mobile) issues. It could also be that Big Data technologies are not sufficiently distinguishable from other technologies to warrant a separate exposition. There are no Big Data cases to analyze. No legislation has been passed that appreciates the dynamics of Big Data, and in particular,

the collection, use, disclosure, and storage of vast amounts and types of data. Lastly, it could be that due to the newness of Big Data, an opinion has yet to form. This will change. The remainder of this article will thus describe current legal developments related to Big Data and suggest potential developments as the courts and legislatures grapple with issues related to Big Data.

As intimated above, in the case law Big Data is still firmly in the hands of the early adopters. In fact, my research revealed only one case that so much as even mentions Big Data:

> First, in the era of 'big data,' in which storage capacity is cheap and several bankers' boxes of documents can be stored with a keystroke on a three inch thumb drive, there are simply more documents that everyone is keeping and a concomitant necessity to log more of them.

Chevron Corporation v. The Weinberg Group, Misc. Action No. 11-409, D.D.C. Sept. 26, 2012. While there are no Big Data cases, geo-location tracking cases, of which there is no shortage, come the closest and shed the most light on Big Data issues. As detailed below, the case law, which involves data collected from attached GPS devices, GPS chips in mobile phones, and cell site towers, is mixed, but generally reflects a reluctance to address issues related to rapidly-changing and potentially invasive technologies. With Big Data, the elephant in the room is, of course, privacy; and while there are other issues, as discussed below, privacy, deservedly, crowds them out. In *United States v. Antoine Jones*, 132 S. Ct. 945 (2012), five Justices, led by Justice Alito, appeared to agree that prolonged monitoring of a person's whereabouts for most offenses would violate a person's reasonable expectation of privacy and, thus, absent a warrant or exigent circumstances, such monitoring would be unconstitutional. However, the case was ultimately decided on a common law trespass analysis, given that a GPS device had been attached to the undercarriage of Jones' car, whose location was tracked for 28 consecutive days. During this period, the GPS device collected more than 2,000 pages of data. The Court's conclusion left unanswered several questions that are important in an era of Big Data. For example, what sorts of offenses would be sufficiently serious to warrant a 28-day search? If 28 days is too long, what about three days or 10 days, and does the granularity of the location data matter? Put otherwise, the "reasonable expectation of privacy" test first articulated in *Katz v. United States*, 389 U.S. 347 (1967), may become increasingly difficult to apply, especially as technologies and our expectations of privacy evolve.

In particular, the "reasonable expectation of privacy" test comes from Justice Harlan's concurring opinion:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'

Katz involved wiretapping a phone booth, and thus eavesdropping on at least Katz's end of the conversation.

In *United States v. Skinner*, 690 F. 3d 772 (2012), the defendant was tracked for only three days, as his GPS-enabled cell phone was pinged periodically to determine location, and to ultimately apprehend him. There, the Court of Appeals for the Sixth Circuit found no Fourth Amendment violation because "Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone" that was used to transport contraband. In reality, GPS-enabled cell phones need to be pinged (by the phone company) to provide data about their location. Similarly, whether or not the phone was used in support of an illegal activity (transporting contraband) should have no bearing on the reasonable expectation of privacy. Judge Donald, in her concurring opinion, agreed to as much, but concluded that the location data evidence should not be suppressed, because a good faith exception to the warrant requirement existed in the case. En banc review by the Sixth Circuit has been petitioned.

At issue in *In re Application of the United States of America for Historical Cell Site Data*, argued on October 2, 2012, in the Court of Appeals for the Fifth Circuit, was 60 days' worth of historical cell site data, which could be used to determine the location of certain individuals in the underlying investigations. While oral argument was generally not terribly illuminating, the court was especially uneasy about the types of data, above and beyond the location of cell site towers at the beginning and end of each call, that would be divulged to law enforcement if the proposed Section 2703(d) order had in fact been granted. One of the critical issues, or side effects, of Big Data is this uneasiness about the collection of vast amounts of data about each person and not knowing what one will find when one opens Pandora's box. Further, the court did not seem eager to decide the Fourth Amendment issue. Rather, it seems more likely that the court will dispose of the case by ruling that Section 2703(d) of the Stored Communications Act (18 U.S.C. §§ 2701-2712), also at issue in this case, compels the issuance of an order once certain information is presented to the magistrate. At any rate, it is only a matter of time before the U.S. Supreme Court weighs in on the collection and use of mobile phone geo-location data and applies, as it must, *Katz* to the facts of the specific case. Further, given the rapidly-evolving technologies and the inherent squishiness of "reasonable expectation of privacy," a bright-line rule seems highly unlikely.

In "The Dead Past" (64 Stan. L. Rev. Online 117), Chief Judge Kozinski, of the Court of Appeals for the Ninth Circuit, questions how much today's society really values its privacy. He surmises:

> In a world where you can listen to people shouting lurid descriptions of their gall-bladder operations into their cell phones, it may well be reasonable to ask telephone companies or even doctors for access to their customer records.

In other words, the goal post keeps moving, and even if a court faithfully applies *Katz*, the application will likely be troubling to a significant minority of us. The application will also likely be quite fact-specific, raising the question if, with respect to at least this aspect of Big Data, whether or not a legislative solution would be preferable. As a simple example, if the law was to expunge historical cell site data after, e.g., 12 months, there would be no *In re Application of the United States of America for Historical Cell Site Data*. Currently, there is no limit on how long phone companies can keep cell site data.

Of course, not using a cell phone is not an option, although, quite tellingly, one of the judges on the Fifth Circuit panel that heard *In re Application of the United States of America for Historical Cell Site Data* asked if the defendants simply could have not used their phones.

The Legal Landscape: Other Issues

There are other issues, such as data security and intellectual property rights, but for the most part, they are more data issues than Big Data issues. In analyzing such data issues, the practitioner should consider the entire data life cycle, which consists of data generation, transfer, use, transformation, storage, archival, and destruction. Consideration should also be given to the nature of the data, gateways (discussed below), business sector-specific laws and regulations, and the location of the consumer or data subject. In short, regardless of whether a certain technology or business practice raises a Big Data issue, the practitioner will still need to consider and analyze data issues raised by the relevant technology or practice.

Gateways, or devices through which data is collected, are critical. For example, earlier this year, California's attorney general announced that apps that collect personal data from California consumers must have a conspicuously posted privacy policy. On September 12, 2012, Representative Edward J. Markey (D-Mass.) introduced the Mobile Device Privacy Act (H.R. 6377), which mandates the disclosure of monitoring software installed on a mobile device or downloadable to such a device, the types of information that may be collected by such software, the recipients of such information, how such information will be used, and procedures to stop further collection of such information. The concept, though, is still notice and consent. Put otherwise, H.R. 6377 will not have any real impact on how much data is collected and for how long it is stored, thus sidestepping some of the major issues raised by Big Data. Further, and perhaps of greater interest (at least to those steeped in information security), the draft bill has rather detailed information security requirements for anyone who receives information collected by monitoring software, including a security policy, the identification of a security officer, and a process for identifying any reasonably foreseeable vulnerabilities in any system containing such information.

More broadly, the nature of the data is, of course, critical. Is the data PII (personally-identifiable information), and if so, is it from or relating to a child under 13, thus invoking COPPA? Likewise, does the data constitute PHI (personal health information), thus invoking the HIPAA Privacy Rule and the HIPAA Security Rule. PII would, of course, subsume PHI, and this is relevant, at least in part, because there is no private cause of action under HIPAA. As to the location of the data subject, the EU justice commissioner, Viviane Reding, has said that it should not matter where data is processed if EU privacy laws are violated. Jurisdictionally, this seems problematic, absent an office or data processing equipment in Europe, but, at any rate, if EU consumers are being actively targeted by a non-EU company, such a company should comply with, e.g., the EU Cookie Directive, and, in particular, the specific implementation adopted by the Member Countries whose consumers are being targeted.

Data generation speaks to the provenance, or source(s), of the data. Issues include the sufficiency of intellectual property rights in the data and whether or not the data was procured in such a way as to not invade a third party's privacy rights or violate a third party's publicity rights. Particular care should be taken by the customer in reviewing API (application program interface) licenses, to determine any limitations on data distribution. For example, some licenses may permit distribution only if the third-party data is accessed dynamically. While it is debatable whether or not APIs are copyrightable, the provenance analysis should still take into consideration the distribution (and other) limitations of the API license.

If the data will be entrusted to a third-party service provider, care must be taken to address permissible use(s) of customer data by the provider, the ownership of any intellectual property attributable at least in part to use of customer data, whether or not the customer data will be treated as customer confidential information, and the commercially reasonable security practices actually implemented and maintained by the provider. Other topics for consideration include the location of the data center(s) in which the data will be stored, whether or not there are any export controls with respect to the data, data quality, the ease with which the data may be accessed and transferred to another service provider, and whether or not there are any attendant costs, and the retention period for the data. Note that security, export control, data quality, and other issues do not disappear if the data is processed and stored internally.

The Road Ahead

While the legal implications of business models that address Big Data have yet to be analyzed extensively by the courts, with the exception of the cases discussed

above and perhaps other disputes dealing with geolocation services, businesses can expect that similar issues will come before the courts soon, as they start to grapple with how people are starting to capitalize on Big Data. Some of the other contexts in which practitioners should expect Big Data issues to play a big part in disputes may include the following:

- Consumer privacy complaints or other third-party complaints against data analytics services that provide data tied to e-mail addresses;
- Other analytics services that provide "analytics" from cloud-based data, regarding customer behavior; and
- Products and services responsible for analyzing, managing, and storing critical and highly complex and sensitive data, such as genomic data.

Conclusion

In closing, while, on the business side, the case for Big Data has been largely fleshed out, the legal ramifications remain to be elucidated. In the short-term, geo-location tracking cases will likely provide the most insight into whether the resolution of Big Data issues will be via judicial fiat or legislation. Regardless, the practitioner should be sensitive to Big Data issues and take a data-centric view of his or her client's products and services, as well as the products and services the client hopes to acquire.

John Pavolotsky's practice focuses on technology transactions and other intellectual property matters at Greenberg Traurig, where he is of counsel. All views expressed herein are solely those of the author and should not be attributed to Greenberg Traurig.

BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

Property Rights in IPv4 Numbers: Recognizing a New Form of Intellectual Property

By Ernesto M. Rubi

It's a fundamental concept in network communications: A message has at least one sender and one receiver. On the Internet, in order for web browsers everywhere to find a user's desired content, something more than an URL is needed: a globally unique identifier called an "IPv4 number" that maps the domain name to the hosting web server. Each website, smart phone, DSL router, and tablet must be assigned one of these numbers in order to reach other devices or content on the Internet. When an IPv4 number (or "number") is assigned to a particular device it becomes an "IPv4 address" (think millions of "Internet homes" sprouting up every second on the web as each device powers on). Crucially, however, only a little over four billion IPv4 numbers are available in the communications protocol (TCP/IP). This means that at any given point in time only four billion simultaneous IPv4 addresses can be routed on the Internet. With today's multiplicity of Internet-connected devices per person, that number is clearly not enough. While the Internet is theoretically limited in size by its four billion-address threshold, its actual growth, appears to have no end in sight.

Naturally, the question emerges: How have users, past and present, obtained these numbers? Certainly, users like you and me obtain these numbers from our Internet service providers (ISPs: i.e., Comcast, our enterprise networks, etc.). The question is better understood from the ISP or enterprise perspective: How do network access providers obtain their IPv4 number distributions?

In the early days of the Internet, universities, corporations, and ISPs were given large sets of numbers by the National Science Foundation or its agents, without restrictions or contractual agreements. ("Hey, Bell Labs, here are 16 million numbers for you to try our new toy we're calling 'NSFnet.'") These early IPv4 numbers are now referred to as "legacy IPv4 numbers" and those who hold them are known as "legacy holders."

Today, however, the process is much more formal. ISPs obtain their numbers from five globally-separated "regional Internet registries" (RIRs) by entering into contractual agreements concerning a certain number range called a "block." RIRs were formed starting in the mid-1990s and today serve as the main source of IPv4 number blocks while also maintaining directory databases somewhat similar to the root domain name servers, ensuring that no IPv4 number is assigned twice. In other words, the core responsibility of RIRs is to process requests from ISPs for IPv4 numbers and to ensure the global-uniqueness of assigned IPv4 numbers through the operation of the RIR number registries. In North America, the registry performing this task is the American Registry for Internet Numbers (ARIN), incorporated in Virginia as a business league in 1997. The other four include LACNIC (Central and South America), AfriNIC (Africa), RIPE (Europe), and APNIC (Asia-Pacific). ISPs having received their IPv4 numbers from RIRs are referred to as "non-legacy holders."

A close analysis of the legacy and non-legacy holder dichotomy reveals an unsettled and widely divergent legal landscape with respects to the rights of these actors over their IPv4 numbers. Two key questions serve to frame the inquiry. First, what legal rights do early (legacy) holders have in their numbers (the answer affects approximately 1.9 billion numbers or 44 percent of the total IPv4 number scope)? Second, what legal rights, if any, do RIRs have over the numbers themselves and where do RIRs base their authority to assign IPv4 numbers to those that request them?

Further compounding the complexity of issue is the urgent reality confronting ISPs the world over: The supply of available IPv4 numbers has been exhausted. RIRs have announced that, in light of current

demand, they have only a few months' worth of unallocated IPv4 numbers. This raises the very real scenario that in a short time anyone seeking to connect to today's Internet will be unable to do so. Network engineers and international telecommunications standards committees have been forecasting this IPv4 exhaustion doomsday for well over a decade. Extensive work has gone to cement next generation technologies such as "IPv6," which will greatly expand the size of the available number inventory. Unfortunately, at last count, less than 1 percent of all Internet traffic worldwide is IPv6. Indeed, many of today's devices – especially those running older hardware and software – are incompatible with IPv6. Bridging IPv4 and IPv6-enabled communications requires a great deal of engineering effort, and this translates into a greater financial burden in the form of hardware and human capital expenditure for those attempting to bridge the number gap.

Consider the following scenario: With a set of legacy IPv4 numbers larger than it currently needs and motivated by a market created due to IPv4 scarcity, Enterprise A elects to lease or sell its IPv4 numbers directly to Enterprise B, a corporation that foresees significant growth in its global network footprint. This marketplace interaction is difficult (if not impossible) today, given the restrictive covenants and policy positions of the various RIRs. Instead of a normal process whereby a seller and buyer engage in private negotiations and thereby define the terms of an IPv4 sale and subsequent agreement, RIRs have sought to place restraints on transfers of non-legacy, and even legacy, IPv4 numbers, insisting on being officious intermeddlers in the business affairs of private and public entities alike. In fact, the RIRs themselves have no legal claim of right over legacy IPv4 numbers, and the restrictive framework that now exists will undoubtedly erode, eventually to disappear. Indeed, the current unworkable RIR policies and registration contracts belie the marked potential for the monetization of IPv4 numbers (both legacy and non-legacy) and the next form of generation of intellectual property assets.

The Nortel Sale – A New Paradigm

In a recent blow to the current RIR policies, Nortel Networks, whose U.S. subsidiary was incorporated in Delaware, filed a voluntary bankruptcy petition in the United States Bankruptcy Court for the District of Delaware under Chapter 11 of the U.S. Bankruptcy Code. Nortel made the decision to treat its IPv4 numbers as an asset and listed them for sale.

Indeed, in late 2010, Nortel began actively marketing its legacy IPv4 numbers. Interest in the IPv4 number assets was strong, with more than 80 potential purchasers identified and seven bids officially submitted for either all or part of the legacy IPv4 number blocks offered for sale. Pursuant to its fiduciary duty as debtor-in-possession, Nortel selected the "highest and best offer for the assets," an offer submitted by Microsoft Corp., with subsequent negotiations resulting in a final agreement to sell all of Nortel's legacy IPv4 numbers. The purchase agreement called for the sale of 666,624 numbers for $7.5 million, a price of $11.25 per number.

After the bankruptcy court ratified the agreement, however, ARIN sought to intervene and submitted "informal comments" to the buyer, Microsoft, which resulted in an amended and restated asset sale agreement between Microsoft and Nortel. Nortel submitted the amended agreement to the bankruptcy court, implicitly calling on the court to decide whether the IPv4 numbers constituted assets capable of being alienated in the same manner as tangible or other intangible assets are disposed of during bankruptcy proceedings. The court ratified the sale.

In the resulting order, the court recognized Nortel's property interest in its legacy numbers. The court held that Nortel had an exclusive right to use the legacy numbers. The court also explicitly sanctioned Nortel's exclusive right to transfer its exclusive right to use the numbers. In recognizing Nortel's exclusive right to *use* legacy IPv4 numbers, the court implicitly found that Nortel had the exclusive right to *possess* the numbers themselves. Consequently, Nortel could exclude others from possession and use of the same legacy IPv4 numbers. In other words, the court found Nortel possessed the customary "bundle of rights" commonly associated with the ownership of tangible or intangible property.

The court's opinion (*In Re: Nortel Networks, Inc. et al.,* D. Del., Case No. 09-101138 (KG)) constitutes an important first step towards the full recognition of a legacy holder's property rights in their IPv4 numbers. After *In re Nortel,* legacy holders can likely succeed in making the case that they, like Nortel, have the exclusive right to transfer their right to use legacy IPv4 numbers. This is effectively the legacy holder's legal right to dispose of its property (the IPv4 numbers) by transfer or sale. By finding that Nortel had all of the rights appurtenant to property ownership in its legacy IPv4 numbers, the court paved the way for future bankruptcy debtors to treat IPv4 numbers as assets that can be offered for sale.

A Deterrent to Marketplace Interaction

Today, ISPs cannot provide Internet access to their downstream customers (i.e., home DSL users) without first themselves accessing the RIR's registries. (For a more in-depth discussion of antitrust issues in the context of RIRs see Rubi, Ernesto M., "The IPv4 Number Crisis: The Question of Property Rights in Legacy and Non-Legacy IPv4 Numbers," 39 AIPLA Q.J. 477 (Fall 2011)). To comply with the various technical imperatives of network routing, including global uniqueness of each IPv4 number advertised, each ISP must check that the numbers received from their network neighbors do in fact belong to the network (AS number) from where they are being received. To do this, they turn to the RIR's registries. However, being listed on the RIR's registries is not

free and accessing the registry's listings has many strings attached.

RIRs require ISPs seeking non-legacy numbers to execute a Registration Services Agreements (RSAs). Only when this agreement is signed do RIRs issue the IPv4 numbers to the registrant from their respective "unallocated number pool" and proceed to register the numbers in its registry. Likewise, RIRs will steer legacy holders into a Legacy Registration Services Agreements (LRSA). The key, however, is that both LRSAs and RSAs are contracts containing clauses purporting to extinguish any property rights (and therefore limit the use and transferability) of legacy and non-legacy IPv4 numbers alike.

LRSAs purport to reaffirm the RIR's control over legacy numbers obtained and used by the registrant prior to the RIR's own existence. Further, LRSAs purport to extinguish *a priori* unencumbered legacy IPv4 numbers' property rights. They do so through the incantation a "No Property Rights" clause, ostensibly forcing legacy holders to give up claims to title and other interests in exchange for registration services from RIRs. To be sure, the identical "No Property Rights" clause is found on both the LRSA and RSA. North American legacy holders, faced with ARIN's LRSA, are presented (and expected to accept, without revision) the following provision:

> Legacy Holder acknowledges and agrees that: (a) the number resources are not property (real, personal, or intellectual) of Legacy Holder; (b) Legacy Holder does not and will not have or acquire any property rights in or to any number resources for any reason, including but not limited to, by virtue of this Legacy Agreement or the prior issuance of any number resources to it or any access or use thereof by Legacy Holder; (c) Legacy Holder will not attempt, directly or indirectly, to obtain or assert any patent, trademark, service mark, copyright, or any other form of intellectual, proprietary, or property rights in any number resources in the United States or any other country; and (d) Legacy Holder will transfer or receive number resources in accordance with the Policies.

See www.arin.net/resources/agreements/legacy_rsa.pdf. The impact of agreeing to such a broad limitation is potentially catastrophic in the face of today's IPv4 number scarcity, the potential property rights legacy and non-legacy holders alike hold in their numbers, and the dearth of authority on the issue of just what legal rights RIRs have, if any, over both types of IPv4 numbers. It is clear that both legacy and non-legacy holders forego their IPv4 number property rights at their own risk.

To be sure, ARIN's LRSA and RSA remain untested in court. However, even a cursory analysis of both RSAs and LRSAs reveals that they are vulnerable to attack under multiple contract theories, including the likely contention that both are nothing more than illusory contracts. Indeed, ARIN's (and the RIR's) apparent promises have qualifications and limitations so strong (and reserve such wide discretion) that they negate the promises contained in the contract itself. *See* Restatement (Second) of Contracts §77. ARIN, as apparent promisor, makes no binding commitment at all. In short, through the RSA and LRSA, RIRs retain an unlimited right to determine the nature or extent of its performance.

Crucially, in the case of non-legacy holders, the RIRs reserve the right to revoke IPv4 number allocations and registration services, but make no mention of providing prior notice. For example, if ARIN determines (and it's unclear how the determination takes place) that a registrant's numbers are not being used in compliance with the terms of the RSA or LRSA, then ARIN reserves the right to revoke and reclaim the numbers from use. (Just how ARIN would "revoke" IPv4 numbers remains to be seen). RIRs also retain the option of discontinuing their performance at their complete discretion. Thus, taken to their logical conclusion, these RSA and LRSA clauses would afford RIRs the private law right to revoke a block of IPv4 numbers and extinguish the Internet presence of private and public actors alike (not even Apple or the U.S. Department of Defense would be immune), for a petty failure to pay the RIR the "yearly renewal fee" of a few hundred dollars.

A Post-RSA/LRSA World

A recent development lends weight to the proposition that the RIR's authority and that of the RSA and LRSA contract is eroding. In a letter dated August 30, 2012, Lawrence Rudolph, general counsel for the National Science Foundation (NSF), formally addressed a request by a private enterprise for guidance concerning its rights to a block of legacy IPv4 numbers. (A PDF version of the letter is available at http://bit.ly/TP8SaA). The request was directed at the NSF, given its stewardship of IPv4 numbers at the very early stages of the Internet. While declining to directly provide legal advice to the private entity, Mr. Rudolph succinctly described the early stages of IPv4 number allocations, painting a picture of the pre-RIR landscape that reveals the recognition by U.S. government entities that IPv4 numbers are "a thing of value." ("NSF transferred 'a thing of value' to the awardee . . . and that awardee in turn gave it to you.")

Importantly, the NSF's letter confronts the latent concern of legacy IPv4 number holders that RIRs, such as ARIN, may be able to "unilaterally reclaim" early number allocations (legacy blocks) and unequivocally rules out such a scenario. In doing so, Mr. Rudolph casts serious doubt on ARIN's authority to issue or enter into RSAs and LRSAs by explicitly stating: "The NSF has never had a cooperative agreement, or any other agreement, with ARIN or any other similarly situated entity." In what is a crystal clear "emperor has no clothes" moment, Mr. Rudolph states: "In short, NSF does not believe that ARIN, or for that matter any other organization [RIRs] could retroactively affect property and rights distributed to you (or any other recipient) by awardee NSI

under its Cooperative Agreement with the [NSF]." To be sure, the NSF's letter is not binding legal precedent but it clearly lends support and the U.S. government's *imprimatur* to the emerging trend that property rights exist in IPv4 numbers ("they are a thing of value"), and casts doubt on the RIR's ability to be the self-appointed arbiters of all things IPv4 – in fact, careful readers will no doubt interpret the letter as an invitation to probe the RIR's legal authority to require RSAs and LRSAs and as a challenge to the monopolization of the IPv4 number allocation and registration function.

Indeed, recognizing property interests in IPv4 numbers and discarding the cumbersome and restrictive RSA and LRSA model would help nascent global enterprises and emerging economies gain a foothold in the ever-growing Internet arena while creating a global marketplace for IPv4 numbers where the monetization of these assets would be possible. The open exchange of legacy and non-legacy IPv4 numbers would allow developing nations and their Facebook-thirsty netizens a viable path to bridge the digital divide. By providing underserved new entrants with enough IPv4 numbers to connect to the current Internet while the necessary investments for IPv6 deployments are worked out, IPv4 markets can promote uninterrupted economic growth. The alternative – curtailing IPv4 number transfers – would provide post-exhaustion IPv6-only entrants access to no more than 2 percent of today's Internet, while forcing them to adopt untested and newer (more expensive) hardware and software. The advantage of an open exchange of IPv4 numbers also goes beyond the financial implications of such transactions, and extends to a basic benefit of Internet connectivity: The emergence of a social and business fabric of innovation and advancement.

Conclusion

The recognition of IPv4 number ownership is inevitable and beneficial. RIRs should not be allowed by their members, or non-members, to stifle competition or delay this inescapable reality. *In re Nortel,* the Microsoft/Nortel multi-million dollar transaction, and the recent NSF general counsel's opinion letter suggest that legal, business, and government interests are aligned in recognizing IPv4 numbers as property and classifying them as outright assets. In the coming post-exhaustion world there will be an unquestionable need to produce new entrants to the Internet landscape. The best solution is to allow IPv4 number holders to freely alienate their number assets. It is time to call these "holders" by the correct title – "owners." Ownership will also likely lead to a more robust global network by promoting the stability of the worldwide Internet, creating incentives for owners of IPv4 numbers to closely monitor and regulate global routing advertisements, and preventing today's frequent address hijackings. As we move forward, large Internet stakeholders such as ISPs, enterprises, and universities will surely recognize their IPv4 numbers as assets. Given the inescapable size limitation on the current IPv4 Internet and the slow adoption of next generation technologies such as IPv6, the conclusion is evident: IPv4 numbers must be free from their static bounds. The world.com depends on it.

Ernesto M. Rubi is an associate at the Miami office of Carey Rodriguez Greenberg & O'Keefe LLP.

BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

Keeping Current:

Plaintiffs' New Racket: Enjoin the Annual Meeting

By Bruce G. Vanyo, Richard H. Zelichov, and Christina L. Costley

Nobody can accuse the plaintiffs' shareholder bar of suffering from a lack of creativity. Congress enacted the Dodd-Frank Wall Street Reform and Consumer Protection Act in July 2010. Section 951 of Dodd-Frank requires a shareholder advisory vote on executive compensation (a "say-on-pay" vote). The Dodd-Frank Act, however, specifically provides that the say-on-pay vote (1) "shall not be binding on the issuer or the board of directors," and (2) does not "create or imply any change to the fiduciary duties of the board members." 15 U.S.C. § 78n-1(c). Nonetheless, following implementation of the law, the plaintiffs began filing derivative lawsuits alleging breach of fiduciary duty following negative say-on-pay votes. All but one of these cases was dismissed because the plaintiff failed to make demand on the company's board of directors before bringing suit. *See , e.g., Gordon v. Goodyear*, 2012 WL 2885695, *10 (N.D. Ill. July 13, 2012) (collecting cases).

The plaintiffs' bar has thus resorted to a new attack: Filing class action lawsuits to enjoin the say-on-pay votes based on allegedly incomplete and misleading proxy disclosures under Delaware law. In many cases, they also add allegations that the proxy statements omit information regarding votes to increase the number of shares available for issuance under a company's certificate of incorporation, votes to increase the number of shares authorized or reserved in connection with equity incentive plans, and votes setting performance goals to obtain tax deductible status for executive compensation under IRC § 162(m).

Plaintiffs' Modus Operandi

Plaintiffs have begun noticing investigation as soon as companies release their proxy statements. Plaintiffs have noticed more than 40 investigations in the last two months, all looking for a stockholder willing to serve as a named plaintiff. As of October 26, 2012, counsel had found stockholders to bring suit in 20 cases; though, of note, counsel appears to be using serial plaintiffs (a single stockholder who repeatedly serves as plaintiff for the same firm) in many of these cases.

The lawsuits share certain common characteristics. For the most part, plaintiffs bring suit: (1) based on purported omissions of material information in a company's proxy statement, not as an attack on the merits of the underlying actions; (2) for injunctive relief, not damages; (3) as putative class actions, not derivative actions; and (4) in the company's principal place of business, not Delaware.

The Claims

In connection with the say-on-pay vote, the complaints generally allege that the following additional information should have been disclosed:

- A "fair summary" of the compensation consultant's analysis provided to the company's board of directors.
- The reasons that the company selected and/or changed its compensation consultant.
- The reasons that the company selected the particular mix of salary, cash incentive compensation, and equity incentive compensation.
- The reasons that the company selected particular companies as peers for purposes of benchmarking executive compensation.
- Details concerning financial and/or compensation metrics concerning the peer companies.

In connection with votes to increase the number of shares available for issuance under equity incentive plans, the complaints generally allege that the following additional information should have been disclosed:

- A "fair summary" of any compensation consultant analysis provided to the company's board of directors.
- Any projections considered by the company's board of directors concerning shares to be granted under equity incentive plans in the future.
- The reasons that the company deter-

mined the number of additional shares requested to be approved for issuance.

- The potential equity value and/or cost of the issuance of the additional shares.
- The potential dilutive impact of the issuance of the additional shares.

Defenses

Because these cases are fairly new, the plaintiffs' bar has seized the opportunity to frame the terms of the litigation. For the most part, plaintiffs are bringing these as claims for "material omissions," which – if taken at face value – makes it difficult (though not impossible) to obtain dismissal at the pleading stage, because materiality is ordinarily viewed as a matter for the trier of fact. *See Matrixx Initiatives, Inc. v. Siracusano*, 131 S. Ct. 1309. As a result, many defendants have been answering the complaints, instead of moving to dismiss, even following decisions by the courts denying expedited relief.

It is a mistake to allow plaintiffs to seize control of the discussion and frame the analysis only in terms of materiality. Plaintiffs have specifically stated they are not bringing suit under Rule 14a-9 of the Securities Exchange Act of 1934 (if they were to do so, the cases would be removable to federal court and subject to the Securities Litigation Reform Act's mandatory discovery stay). Instead, they bring suit under Delaware law based on alleged violations of the duty of candor, a duty recognized by the Delaware Supreme Court in *Malone v. Brincat*, 722 A.2d 5, 10 (Del. 1998). *Malone* has been interpreted by the Delaware Court of Chancery as requiring plaintiffs to plead and prove all the elements of common law fraud, including: (1) material misrepresentations; (2) intent to deceive; (3) reliance; and (4) damages. *See Metro Communication Corp. BVI v. Advanced Mobilecomm Technologies Inc.*, 854 A.2d 121, 131–32 (Del. Ch. 2004) (noting that the Supreme Court in *Malone* required plaintiffs to "show reliance and scienter" so that Delaware does not "encourage a proliferation of disclosure claims"). We believe that, when plaintiffs bring suit for a breach of the *Malone* duty, it is critical to hold them to the heightened standards for pleading and proof set forth by the Delaware courts in interpreting *Malone*.

It is an error to allow plaintiffs to characterize these claims as direct disclosure violations; rather, the claims should be considered derivative. A derivative claim belongs to the corporation and can be brought by a stockholder only if he or she first pleads specific facts establishing that the shareholder has either made a demand for litigation on a company's board (and the demand has been wrongfully refused) or that demand is excused. The proxy disclosure claims are derivative because any harm suffered by a less than fully informed say-on-pay vote or the authorization of excessive options is a harm suffered by the corporation itself and is actionable only as a claim for waste or dilution. *See Feldman v. Cutaia*, 951 A.2d 727, 732 (Del. 2008) (claims for dilution and based on a failure to disclose material information in connection with a vote on an employee stock option plan are derivative); *Abrams v. Wainscott*, 11-297-RGA, 2012 WL 3614638, *3 (D. Del. Aug. 21, 2012) (executive compensation disclosure claims are derivative). Further, because the facts alleged are properly cognizable only as claims for waste or dilution, the claims are not ripe until the defendant boards actually issue compensation or shares following the votes.

Looking Forward

Plaintiffs have had limited success on these cases. A plaintiff obtained an injunction stopping a shareholder vote by Brocade Communications Systems, Inc., on increasing the number of shares available under an equity incentive plan and was awarded attorneys' fees of $625,000. Plaintiffs have obtained settlements in cases involving H&R Block, Martha Stewart Living Omnimedia, Inc., NeoStem, Inc., and WebMD, LLC for amounts between $125,000 and $450,000. In contrast, plaintiffs voluntarily dismissed a case against Amdocs after defendants opposed the preliminary injunction motion and moved to dismiss and plaintiffs also failed to enjoin shareholder meetings of Ultratech and AAR.

Despite plaintiff's mixed results, as companies with calendar year-ends enter the 2013 proxy season, filings are expected to accelerate. Plaintiffs, in general, have had more success on claims involving stock issuance than on claims involving just say-on-pay votes, and likely, moving forward, the plaintiffs will focus the lawsuits accordingly. Further, if the heightened burdens discussed above are adopted by the courts, plaintiffs may find it more economical to select their claims with more care.

Bruce G. Vanyo and Richard H. Zelichov are partners, and Christina L. Costley is an associate at Katten Muchin Rosenman LLP.

BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

Delaware Insider:

The Application of Default Fiduciary Duties to Delaware Alternative Entities: The Saga of Uncertainty Continues

By Dominick Gattuso

In January 2012, the Delaware Court of Chancery issued a decision in *Auriga Capital Corp. et al. v. Gatz Properties, LLC*. The decision caught the attention of practitioners within and without Delaware, because the Court definitively ruled that traditional fiduciary duties of care and loyalty apply by default to managers of Delaware limited liability companies absent a contractual provision that clearly alters or eliminates such duties. While numerous decisions from the Court of Chancery over the years suggested as much, *Auriga* was the first instance where the Court made an unequivocal pronouncement. On appeal, the Delaware Supreme Court, acting *en banc*, affirmed the trial court's award of damages and attorneys' fees, but squarely rejected the "court's pronouncement that the Delaware Limited Liability Company Act imposes 'default' fiduciary duties on upon LLC managers and controllers unless the parties to the LLC Agreement contract that such duties shall not apply."

The dispute in *Auriga* centered on the acquisition of Peconic Bay LLC by Gatz Properties, LLC (Gatz Properties), which was the company's sole manager, and which held majority voting control in Peconic Bay. Defendant William Gatz (Gatz) and certain of his family members owned and controlled Gatz Properties, which held title to property owned by the Gatz family in Long Island, New York. Gatz Properties leased the property to Peconic Bay under a ground lease with a 40-year term. The ground lease restricted the property's use to a high-end, daily fee, public golf course. In 1998, Peconic Bay sublet the property to American Golf Corporation, which ran the day-to-day operations of the golf course until 2004. Upon learning that American Golf did not intend to renew its sublease, Gatz engaged in a series of actions that placed Peconic Bay in an economically vulnerable position so that he could acquire the company at a steep discount and, thereby, avoid the long-term ground lease that prevented him from developing the property into a private, residential golf course. The *coup de grace* – a "sham" auction to squeeze out Peconic Bay's minority investors – led the investors to sue Gatz and Gatz Properties. The minority investors alleged that Gatz breached both his fiduciary duties and Peconic Bay's operating agreement. Gatz countered that he owed no fiduciary duties, because such duties had been eliminated by the operating agreement.

The Chancery Court began its analysis by answering the question of whether traditional fiduciary duties apply to managers of a Delaware limited liability company affirmatively. His approach was straightforward. Section 18-1104 of the Delaware Limited Liability Company Act, which states, in part, that "[i]n any case not provided for in this chapter, the rules of law and equity . . . shall govern," is more explicit than its corporate counterpart "in making the equitable overlay [of traditional fiduciary duties] mandatory" in the LLC context to the extent that those duties have not been altered or eliminated by the relevant operating agreement. As the court explained, the "manager of an LLC has more than an arms-length, contractual relationship with the members of the LLC." Rather, an LLC manager is "vested with discretionary power to manage the business of the LLC." As such, the manager qualifies "as a fiduciary of that LLC and its members." Because "the rules of equity apply in the LLC context by statutory mandate, . . . because LLC managers are clearly fiduciaries, and because fiduciaries owe duties of loyalty and care," it is only logical that Delaware LLCs start "with the default that managers of LLCs owe enforceable fiduciary duties."

In reaching this conclusion, the court squarely rejected a competing view that fiduciary duties should not apply to LLC managers by default. First, if the Delaware courts "judicially excised" the equitable overlay of fiduciary duties in the statute, "those who crafted LLC agreements in reliance on equitable defaults that supply a predictable structure for assessing whether a business fiduciary has met his obligations to the entity and its investors will have their expectations disrupted." In other words, the "equitable context in which the contract's specific terms were to be read will be eradicated, rendering the resulting terms shapeless and more uncertain." The second problem follows

directly from the first: "Judicial eradication of the explicit equity overlay in the LLC Act could tend to erode [Delaware's] credibility with investors in Delaware [alternative] entities."

The court next considered whether the parties "displac[ed the default] fiduciary duties altogether or tailor[ed] their application, by substituting a different form of review." Peconic Bay's operating agreement contained no provision expressly eliminating default fiduciary duties. Nor were default fiduciary duties displaced by Section 15 of Peconic Bay's operating agreement, as Gatz claimed.

> Section 15 stated: "[N]either a manager nor any other member shall be entitled to cause the Company to enter . . . into any additional agreements with affiliates on terms and conditions that are less favorable to the Company than the terms and conditions of similar agreements which could be entered into with arms-length third parties, without the consent of a majority of non-affiliated members. . . ."

In *Gotham Partners, L.P. v. Hallwood Realty Partners, L.P.*, the Court of Chancery interpreted similar contractual language "as imposing the equivalent of the substantive aspect of entire fairness review, commonly referred to as the 'fair price' prong." The *Auriga* court explained that the "fair dealing" prong of the entire fairness review does not "fall away, because the extent to which the process leading to the self-dealing either replicated or deviated from the behavior one would expect in an arms-length deal bears importantly on the price determination." In other words, Section 15 "distill[s] the traditional fiduciary duties as to the portion of the Minority Members' claims that relates to the fairness of the Auction and Merger into a burden to prove the substantive fairness of the economic outcome." Thus, to enjoy Section 15's safe harbor, and thereby avoid the need for minority member approval of the auction and merger, "Gatz [had] the burden to show that he paid a fair price to acquire Peconic Bay, a conclusion that must be supported by a showing that he performed, in good faith, a responsible examination of what a third-party buyer would pay for the Company." The court reasoned that the remainder of Gatz's alleged misconduct leading up to the auction and merger were "governed by traditional fiduciary duties of loyalty and care because the LLC Agreement does not alter them."

The court held that Gatz breached both his contractual and fiduciary duties to the minority members of Peconic Bay by engaging in a series of acts and omissions over the years that left Peconic Bay in a tenuous financial position, which Gatz exploited "by buying [Peconic Bay] at an auction on terms that were well-designed to deter any third-party buyer, and to deliver the LLC to Gatz at a distress sale price." Because Gatz acted in bad faith, the exculpatory provision in Peconic Bay's operating agreement did not absolve him of monetary liability for his wrongdoing. Accordingly, the trial court awarded the minority members damages in the amount of $776,515 as well as pre-judgment interest at the statutory rate, compounded monthly, until the date of the final judgment. The court also awarded the minority members a portion of their attorneys' fees, finding that Gatz engaged in abusive litigation tactics including asserting implausible factual and legal arguments and destroying relevant documents both during litigation and when litigation was likely.

On appeal, the Delaware Supreme Court identified the "pivotal" legal issue as "whether Gatz owed contractually-agreed-to fiduciary duties to Peconic Bay and its minority investors." The Supreme Court answered the question affirmatively. That Section 15 of the operating agreement did not contain the words "fiduciary duties" or "entire fairness" was inapposite, because there is "no requirement in Delaware that an LLC agreement use magic words" to "impose fiduciary standards of conduct as a contractual matter." The parties in *Auriga* adopted the "contractual equivalent of the entire fairness equitable standard of conduct and judicial review" through Section 15. The Supreme Court reasoned that Gatz's admissions that he owed fiduciary duties and that those duties had not been waived in the operating agreement confirmed their contractual interpretation. The Delaware Supreme Court affirmed the trial court's finding that Gatz breached his contracted-for fiduciary duties to the minority members of Peconic Bay, and agreed that Gatz was not entitled to exculpation by virtue of the exculpatory language in Section 16 of the operating agreement, because "he had acted in bad faith and had made willful misrepresentations in the course of his breaching his contracted-for fiduciary duty." Accordingly, the Supreme Court affirmed the Chancery Court's award of damages and attorneys' fees to the minority members.

However, the Delaware Supreme Court took the unusual step of admonishing the Chancery Court for its "unnecessary construction" of Delaware's LLC Act to provide for application of default fiduciary duties. The Supreme Court explained: First, "the dispute over whether fiduciary standards apply could be decided solely by reference to [Section 15] the LLC Agreement. . . ." Second, no party asked the trial court "to decide the default fiduciary duty issue as a matter of statutory law." Indeed, by trial, the parties were no longer contesting the existence of fiduciary duties under the operating agreement. Third, the Supreme Court is not bound by prior decisions of the Court of Chancery, which hold, implicitly or otherwise, that default fiduciary duties apply to managers of Delaware LLCs. Lastly, the Supreme Court noted that the issue – whether the Delaware LLC Act does, or does not, impose default fiduciary duties – "is one about which reasonable minds could differ," and posited that resolution of any "statutory ambiguity on the issue" may be better left to the Delaware Bar and the General Assembly.

Reading the Delaware Supreme Court's decision in *Gatz Properties, LLC v. Auriga Capital Corporation* immediately brought to mind the famous and long-running commercial for Tootsie Pops that began in 1970, where a boy asks a fox, a turtle, and finally an owl "how many licks does it take to get to the Tootsie Roll center of

a Tootsie Pop?" Unfortunately, the owl, like the fox and turtle before it, cannot withstand the temptation to bite through the hard candy exterior in a sugar-fueled rush to get to the Tootsie Roll in the center. So, "[h]ow many licks does it take to get to the Tootsie Roll center of a Tootsie Pop? The world may never know." And so too, the world may never know whether default fiduciary duties apply to managers and general partners of Delaware alternative entities.

Dominick Gattuso is a partner with Proctor Heyman LLP, in Wilmington, Delaware, and practices in the areas of corporate, alternative entity, and commercial litigation. The views expressed herein do not necessarily represent the views of Proctor Heyman LLP or its clients.

Additional Resources

For other materials related to this topic, please refer to the following.

Business Law Today

Is Delaware Alternative Entity Law Cutting Edge or Cutting Loose?

By Dominick T. Gattuso
August 2012

BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

Member Spotlight:

Interview with Marshall Small

By Leslie Gordon

After graduating from Stanford Law School in 1951, Marshall Small clerked for U.S. Supreme Court Justice William O. Douglas and later served as an active duty army officer in the Office of the Judge Advocate General. In 1954, he joined the firm now known as Morrison & Foerster and served in many leadership roles there, including managing partner, general counsel, and chair of the firm, and was an early champion of law firm diversity. Small's corporate practice included negotiating mergers, representing bidders and target companies related to tender offers, counseling boards of directors, and serving as special counsel to board committees.

An Advisor to the ABA's Business Law Section, Small also served on the Section's Committee on Corporate Laws from 1974 through 1982. He was a member of the Subcommittee on Functions and Responsibilities of Directors and helped prepare the original *Corporate Directors' Guidebook*. He's a member of the American Law Institute, a fellow of the American Bar Foundation, and served as a reporter for the American Law Institute's Corporate Governance Project from 1982 through its completion in 1993. A one-time assistant professor at Stanford Law School, he's lectured and written extensively on corporate and securities law. Described by a colleague as a "corporate law genius," Small was awarded the California State Bar Business Law Section's Lifetime Achievement Award in 2002.

Originally from Kansas City, Missouri, Small has been married for 58 years. Amidst his law practice, serving as general counsel to his firm, and his extracurricular work at the ABA and other organizations, Small also served for years as an unpaid teacher's assistant in a primary school in a low-income neighborhood.

What inspired you to attend law school and practice law?

While I was in college at Stanford, I took two law-related courses, one on constitutional law and one on business ethics. Both were very stimulating to me. One professor, in particular, encouraged me to go to law school. As far as practicing, after clerking, I was offered a teaching position on a temporary basis at Stanford Law School – but it was only temporary. I was newly married and I needed to make sure we had a roof over our head and food on the table. So I felt I'd better start practicing law.

What was the primary lesson that you took away from your experience as a U.S. Supreme Court clerk?

I'm not sure whether there was a primary lesson or not. I clerked for William O. Douglas during the '51 term. He was a tough boss – no nonsense when you were working across the desk from him on the Court's work. He was very bright and very quick. You learned to be responsive and responsible. When you were able to deal with him outside of the work at the Court, he could be an interesting, charming person. But it was no nonsense when you were with him at the Court. He relied on you to make sure that you were checking him and doing everything correctly.

What was the primary lesson you learned while serving as a lawyer in the Army JAG Corps?

For one thing, I developed a great deal of respect for the regular army officers. They were very competent professionals. And I was grateful just as a citizen that they were devoting their careers to help the United States. The second thing was the realization that the military recognized the primacy of civilian control of the government, which is very important to a democracy. One task that I was assigned involved the separation of powers. So I spent a fair amount of time down in the Pentagon law library reading the Constitutional Convention debates and I came away with a great deal of respect for the Founding Fathers in terms of the constitution that they hammered out. So those were things I carried with me in my memories.

Why did you specialize in corporate work?

When I joined our firm, it was a midsize firm. I was the twenty-third lawyer. In those days, it wasn't departmentalized and you did a little bit of everything. I started doing corporate work because the firm had

a great deal of corporate work then and they gave me responsibility early on. By the time I was an associate there for two years, I was carrying substantial responsibility. I enjoyed the work. I enjoyed the partners with whom I was working. And so it was just natural that I became specialized on the corporate side of the firm and I never regretted it. I've worked from time to time over the years with litigators on various matters, both tender offer defense work and special board committee work, where we worked as teams. But, basically, during my career, it was specializing in corporate work.

What were your early years in practice like and how does it compare to the practice for young lawyers today?

The research, for one thing, was much more grueling. Document preparation was in the dark ages. Then, you typed with carbon paper. There wasn't such a thing as computers in those days – the way younger lawyers regularly use computers today. As for communication, there was no such thing as e-mail or the Internet. It's just a completely different world. In research and communication, there are so many more things that are available to you now electronically that there weren't then. So I think, in many ways, it's easier to practice as a young lawyer in terms of the tools you have available to help you that you didn't have in those days.

Why has law firm diversity been an important mission for you?

When I came into the practice, things were starting to change. I am of the Jewish faith and law firms were just opening themselves up to people of the Jewish religion at that time. I was the first at our firm in many years. And it was important to me to see that there was a diversity viewpoint in the firm. There were no women lawyers in those days. As matter of fact, there were very few women in law school – I think there may have been three women law students in my law school class. I'd had a strong desire for diversity, going back to the days when I was a teenager in high school and was involved in a community group that made it an effort to see that people of different races and religions were together and got to know each other. During World War II, the leader of the group made an effort to include Japanese Americans. So I carried that experience with me and always looked to build bridges to different types of people. It's been particularly fulfilling and satisfying to see our firm develop into a very diverse firm in the best sense.

Describe what it was like to serve as a general counsel for the firm of which you were a partner.

A firm our size has a thousand lawyers in a number of different offices, including overseas offices, and is a very large institution with lots of issues. One of the things that sets law firms apart when you're acting as counsel to the firm is the fact that they are professional institutions. So professional ethics are one of the things that you're often dealing with, not just conflicts of interest, but the variety of professional ethics issues, like unauthorized practice of law and the partnership agreement. Traditionally in our firm I have been responsible for many years for interpreting and amending the partnership agreement. It's a fairly complicated document now. There are also issues of structure of the various firm entities in the various offices overseas. It's an interesting and challenging task. It's been a very satisfying thing to do after I retired as an active partner to be able to continue to do this and have the firm feel that I could still be useful.

What has been the most fulfilling moment in your work so far?

I don't know that I'd say there was any one fulfilling moment. I had my work on the ABA Business Law Section Corporate Laws Committee, which I found quite fulfilling when I was doing that back in the '70s and '80s. And my work as a reporter on the American Law Institute's Corporate Governance Project, which took from about '82 to '93, I found quite fulfilling and satisfying. On the professional level, my work in advising board committees on special investigations and such and defending take-over targets I found quite fulfilling.

What was a highlight of serving as a Business Law Section Advisor?

I suppose it was the speech I gave to the Council, which is traditional for Business Law Advisors to do. I enjoyed that. I also enjoyed the panel on which I served – it was giving advice to young lawyers about the challenges they would face and how to meet those challenges. Being involved on the Corporate Laws Committee in the Business Law Section really instilled in me a long-term interest in corporate governance and corporate governance trends.

Is there a commonality among the most successful business lawyers that you know?

For one thing, I think you need to treat your opponent, who's on the other side of the table, with respect. And also try to think in terms of what they're trying to accomplish and whether you can build bridges so that you can accomplish what your own client wants to try and achieve and, at the same time, trying to see if you can meet those objectives of the other party to the transaction. Successful business lawyers do that.

Who is your idol in the legal profession?

I'm not sure that I would characterize anyone as an idol, but it was more of in terms of respect. And I'm not sure that there is any one person. It goes back a long way. I watched John W. Davis of Davis Polk argue three cases before the U.S. Supreme Court and I thought he was a consummate appellate litigator. Another is Herbert Clark, a senior litigator when I joined the firm, who was the soul of integrity as well as nationally known litigator. And John Austin and Bob Raven, who were senior partners here.

What are your interests outside of the law?

Reading – mostly nonfiction and history – and gardening and travel. My wife is a

birder so I keep her company when she goes looking for birds and we've been to various places around the world.

Who has been your most influential teacher?

I guess when I come down to it, maybe my most influential teacher was my seventh-grade elementary school teacher because she taught me to really work hard and devote myself to my studies. Before that, I'd been an indifferent student in elementary school. I learned to work hard with her, and I just remember her for that reason.

What is the best idea that you've ever had?

Well, I guess two: Number one, marrying my wife, and number two, joining my law firm, Morrison & Foerster.

What made you pick MoFo among other firms?

I had the feeling that, of the various firms that I interviewed with in San Francisco, they were interested in me as a person. They made sure that I went around and saw almost all the partners in the firm when I interviewed. I had three offers at the time. I chose the Morrison firm and never regretted it.

What is the most unique thing about you?

Well, unique is one-of-a-kind and I don't consider myself one-of-a-kind. But one of the things that may be is interesting is that I'm still working at 85 and enjoying it.

For lawyers who enjoy their work and would like to be involved in the profession as long as you have, well into their eighties, do you have any tips or words of advice?

You need to keep interested in what you're doing. Keep physically active as well. It's very important to be connected with the world. That's the best advice I have. And consider yourself lucky if you have your health and also have the companionship of a good spouse to keep you on your toes.

BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

Inside Business Law

November 2012

Focus on Middle Market and Small Business Committee

The Middle Market and Small Business Committee provides great tools and references for U.S. and international corporate and transactional lawyers who counsel clients ranging from private family and middle market enterprises to smaller public companies on the myriad of business issues they confront in their practices. Be sure to consult the Fall 2012 issue of the *Business Visions Newsletter* published by the Middle Market and Small Business Committee which contains a recap of the ABA's Annual Meeting in Chicago, as well as an update on upcoming meetings. The newsletter contains significant highlights of CLE programming and updates on what to expect this coming year. We look forward to receiving a recap on the articles and topics covered in the upcoming meetings.

Some of the programs co-sponsored by the Middle Market and Small Business Committee at the Annual Meeting include informative presentations on crowdfunding, and the recent impacts of the Jumpstart Our Business Startups Act.

Commercial Law Programs and Content

In the Fall 2012 *Commercial Law Newsletter*, the Commercial Finance and Uniform Commercial Code Committees provide a joint report on the 2012 Annual Meeting and feature several new articles by new contributors. Don't miss out on the following contributions:

- "Using Limited Liability Company Interests and Limited Partnership Interests As Collateral" by Tarik J. Haskins
- "Cybercrime And Online Banking Fraud: An Overview Of The Rules For Allocating Commercial Account Losses" by Salvatore Scanio and Robert W. Ludwig, Jr.
- "Loan Participations – Time For Another Look Part II" by Andrew Connor
- "Are Factoring Transactions "True Sales"? Should Factors Care?" by Haywood A. Barnes

Cyberspace Committee Updates:

It appears that the coming months will be quite busy for the Cyberspace Committee as they have announced packed programs through April 2013 in their Fall 2012 newsletter.

Be sure to read the updates from the International Trade Subcommittee, the Identity Management Legal Task Force, the Digital Media Subcommittee, and the Cloud Computing and IT Services Subcommittee on their current projects.

Business Law Today Board Members 2012-2013

Co-Chairs:

Patrick T. Clendenen
Nelson Mullins Riley & Scarborough LLP
pat.clendenen@nelsonmullins.com

William B. Rosenberg
Stikeman Elliot
wrosenberg@stikeman.com

Advisor:

Robert Boehm
Steiner Leisure Limited
bobb@steinerleisure.com

Members:

Warren E. Agin
Swiggart & Agin, LLC
wea@swiggartagin.com

Miriam R. Albert
Hofstra University School of Law
lawmra@hofstra.edu

Mitchell L. Bach
Eckert Seamans Cherin & Mellott, LLC
mbach@eckertseamans.com

Joan Durocher
National Council on Disability
jdurocher@ncd.gov

Therese G. Franzén
Franzén and Salzano, P.C.
tfranzen@franzen-salzano.com

Jeannie Frey
Resurrection Health Care
jfrey@reshealthcare.org

Karl A. Groskaufmanis
Fried, Frank, Harris, Shriver & Jacobson LLP
karl.groskaufmanis@friedfrank.com

Alicia L. Gutierrez
The Moses Law Firm
alicia@moseslaw.com

Kathleen S. McLeroy
Carlton Fields
kmcleroy@carltonfields.com

Juliet Moringiello
Widener University School of Law
jmmoringiello@widener.edu