Featured Articles

- **Our Mini-Theme: Watches and Wallets, Compliance and Rebellion: The State of Cyberspace Law**

- **Internet Governance Overview: How Snowden Didn’t Really Change Anything After All**
  Revelations by Eric Snowden of the NSA’s extensive surveillance program sent a shock wave through the Internet world, especially for those arguing in favor of not regulating the Internet (i.e., those in favor of a “multi-stakeholder” framework for Internet governance). Then in March of this year, the U.S. Department of Commerce’s NTIA announced it was starting a process to consider transitioning oversight of some technical functions away from IANA over to the “multi-stakeholder community.” All told, it’s been a big year for multi-stakeholderism in Internet governance. What does it all mean?

- **Bitcoin for Merchants: Legal Considerations for Businesses Wishing to Accept Bitcoin as a Form of Payment**
  This article examines the legal risks and issues that a business should evaluate before accepting bitcoin as a form of payment. It provides a brief overview of bitcoin, addresses potential registration and licensing issues, and examines the tax implications of accepting the virtual currency. This article also discusses the use of bitcoin merchant service providers (BMSPs) which act as intermediaries between a business and a customer wishing to pay in bitcoin.

- **Net Gets Physical: What You Need to Know About the Internet of Things**
  The Internet of Things (IoT) has become a hot topic in venues as disparate as consumer electronics shows and government regulatory proceedings. The topic is a big one, and is poised to get much bigger. This article will introduce the IoT and address some of the legal issues that will accompany its growth.

- **The Practical Tech Lawyer: Advising a Company on Data Security Compliance**
  This article will help you understand the broad strokes of danger, complication, risk, and protection for data security in business, health, educational, or governmental entities. Breaking the topic into discrete and practical viewpoints, the article can help the business lawyer better advise clients and minimize risks.
Departments

- **KEEPING CURRENT**: SEC Enforcement Actions Emphasize Importance of Stock Ownership Reporting Obligations for Public Companies and Insiders
  
  On September 10, 2014, the SEC announced charges against 28 officers, directors, and major stockholders of public companies for violating Section 16(a) and/or Section 13(d) of the Securities Exchange Act of 1934. Six public companies were also sanctioned. A total of 33 out of these 34 individuals and companies agreed to settle charges and pay financial penalties totaling $2.6 million. These sweeping actions are another step in the SEC's initiative to "fix broken windows," as described by SEC Chair Mary Jo White in her public remarks on October 9, 2013.

- **DELAWARE INSIDER**: Chancery Court Reaffirms Delaware’s Deferential Approach to Evaluating Fiduciary Claims Brought by Creditors of Distressed Corporations
  
  In its recent decision of Quadrant Structured Products Co. Ltd. v. Vertin, the Delaware Court of Chancery affirmed that Delaware will continue to protect the decisions of directors of an insolvent corporation under the business judgment rule in their pursuit of value-maximizing strategies, so long as the strategy is undertaken based on a good faith and informed belief that it will increase the corporation’s value even if ultimately unsuccessful.

- **ETHICS CORNER**: Be Very Quiet... I’m Hunting Jurors: Social Media and Ex Parte Communications
  
  Very often, proper preparation for litigation demands that we investigate a myriad of parties, and one of the tools at our disposal is social media. Yet investigating potential jurors through social media can throw a monkey wrench into our understanding of the standards for acceptable conduct. A relatively recent opinion from the New York City Bar Association on this topic caused a bit of an uproar in the ethics world. The ABA has also opined on the topic and came down with a contradictory result.

- **MEMBER SPOTLIGHT**: An Interview with Alex Dimitrief
  
  Alex Dimitrief’s story epitomizes the American dream. Not knowing any English, his parents left Russia and immigrated to Montreal, then moved to Illinois. They watched their son attend Yale, where he graduated summa cum laude, then Harvard Law School, where he graduated magna cum laude. He even served as a White House Fellow in the Reagan Administration’s Office of Political and Intergovernmental Affairs, the youngest ever Fellow at that time. Now he is Senior Vice President and General Counsel at GE Capital.

- **INSIDE BUSINESS LAW**
  
  This month’s Inside Business Law highlights several recent Committee meetings and programs, and includes hyperlinks to the written and audio program materials. We also cover highlights from a number of recent BLS Committee newsletters and several upcoming events, including the BLS Fall Meeting and the latest In the Know webinar. Hyperlinks for all these features are provided.
This month’s Cyberspace Law mini-theme in Business Law Today combines the timely and the timeless. Management of the Internet may be in flux, with direct consequences for American business. David Satola and Michael Kelly have been attending the most important recent ICANN meetings and provide an update of a fight for power with all the drama of a telenovela. Steve Middlebrook lends his considerable expertise in payment systems to provide pointers to lawyers whose clients want to use bitcoin for payments. Middlebrook highlights the most practical aspects of the bitcoin phenomenon and places it in the context of our already familiar current payment options.

John Rothchild glimpses the future of Cyberspace Law as he describes our new era of connectivity and automation that some are calling the “Internet of Things.” He finds new and practical legal issues, like the regulation of self-help software options that are already changing the way automobiles are sold and the loans for them are secured. Finally, I add a meditation on the eternal concerns of protecting your most valuable assets. But now, the assets are electronic, and laws, rules, and regulations command you to protect them in specific ways.

Together, these articles demonstrate directions for the future of Cyberspace Law, colored with the split between implementing cutting-edge technology and regulating practical business matters. Enjoy the mini-theme and keep your eyes on this space.

Ted Claypoole is the Chair of the Cyberspace Law Committee.

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

**Business Law Today**
Cyber-Crime, -Cars, and -Coins: Hot Topics in Cyberlaw
(Nov. 2013 mini-theme)

Developments in Cyberspace Law
(Nov. 2012 mini-theme)

Topics in Cyberspace Law
(Dec. 2011 mini-theme)

**ABA Web Store**
RFIDs, Near-Field Communications, and Mobile Payments: A Guide for Lawyers
Apple Pay’s launch makes near-field and mobile payments easier than ever before. More than 200,000 retailers in the U.S. already have near-field readers ready to assist their customers with Apple Pay payments. RFIDs, Near-Field Communications, and Mobile Payments: A Guide for Lawyers covers regulation in the U.S. and abroad and divergent regimes for the protection of consumers’ privacy with regard to this new technology that many companies have adopted.

Internet Law for the Business Lawyer, Second Edition
Internet Law for the Business Lawyer, Second Edition is a great toolkit for advising clients in the electronic environment. The book contains a 10 list of statutes, relevant cases, and regulations, as well as practice tips and important issues when business is conducted in the ever-evolving electronic environment.
Cyberspace Law Institute and Winter Working Meeting

Join the Cyberspace Law Institute and Winter Working Meeting on January 23–24, 2015, at the Omni Charlotte Hotel in Charlotte, N.C. The meeting will include four hours of CLE programs, roundtable discussions and work time, as well as chances to mingle and network. Also expect excellent conversations on cutting edge cyberspace topics with some of the top technology lawyers in academia, government, corporate representation, and private practice. If you’re new to the committee, this is a great way for us to get to know you and your expertise! We look forward seeing you in Charlotte.
A lot has happened in the world of Internet governance this year, starting with revelations by Eric Snowden of the NSA’s extensive surveillance program. That sent a shock wave through the Internet world, especially for those arguing in favor of not regulating the Internet (i.e., those in favor of a “multi-stakeholder” framework for Internet governance). Then in March of this year, the U.S. Department of Commerce’s National Telecommunications and Information Agency (NTIA) announced it was starting a process to consider transitioning oversight of some technical functions, like Internet numbering resources, protocol assignments, and management of domain names, performed by the Internet Assigned Numbers Authority (IANA), away from IANA over to the “multi-stakeholder community.” So although by any measure, it’s been a big year for multi-stakeholderism in Internet governance, what does it all mean?

By way of explanation, multi-stakeholderism refers to the range of actors involved in running, administering, and governing the Internet. It came into popular usage in 2005 as a result of the UN’s World Summit on Information Society (WSIS) which confirmed, inter alia, that “...management of the Internet encompasses both technical and public policy issues and should involve all stakeholders.” As described in the WSIS Agenda, the groups of stakeholders with an interest in Internet governance include governments, the private sector, civil society, intergovernmental and international organizations – viz. the public sector, the private sector, NGOs, academia, the technical community, etc. The multi-stakeholder approach to Internet governance is an accurate reflection of the various actors who together form the loose de facto framework for Internet governance. For example, some of these stakeholders include the Internet Engineering Task Force (IETF), which is not even a formal entity, but which is in charge of the protocols on which the Internet runs. The Internet Corporation for Assigned Names and Numbers (ICANN), the organization that performs technical functions on the Internet (like running root servers – the computers that control traffic on the Internet, and domain name administration (i.e., .com, .org, .gov), is a California not-for-profit corporation. The list goes on.

But the whole notion of multi-stakeholderism and the flexible Internet governance vision it embraces has been under threat. A growing group of countries led by Brazil, Russia, India, and China would prefer that governance of the Internet be centralized and controlled through an inter-governmental (i.e., state-centric) body, such as the UN, the ITU (International Telecommunication Union), or some other, new international organization. This alternative model of Internet governance based on tighter state control is known as multinationalism. While the community of nations supporting multi-stakeholderism comprise mainly Western, wealthier, technologically advanced countries from the developed world, those countries supporting the multinational (i.e., state-centric) approach are mainly developing countries, or countries from the “South” that will use this fight to generally push back against what they perceive as yet another example of Western power dominating an area of international policy. Like the cold war, this tension over multi-stakeholderism had been chugging along for years with no real change to the fairly well-entrenched positions, pro and con.

Then along came Mr. Snowden.

Without getting in to the substance of his revelations, suffice it to say that, in the perception of much of the world, companies that offer services on the Internet were implicated by the Snowdon revelations (Verizon, Google, Facebook, etc.)
were all lumped together with the Internet itself, and for a moment in time, NSA surveillance and the Internet were seen as the same. Accordingly, existing positions for and against a multi-stakeholder Internet governance model became even more polarized. In this context, it seemed a third path might be taken when Brazil suggested a high-level conference, called “NetMundial,” to address management of the Internet in light of Snowden’s NSA surveillance revelations. Trust in the Internet had been undermined. Implicitly, trust in the multi-stakeholder model, and especially in the United States, which through NTIA still exercised a degree of control over the “IANA functions,” was also undermined. However, what began as a challenge to the multi-stakeholder model was at the same time a disappointment to those advocating a more state-centric approach and a relief to those supporting the multi-stakeholder approach. In one of the official documents from “NetMundial,” the conference endorsed an “open and distributed” Internet architecture as well as Internet governance principles including, “a democratic, multi-stakeholder process [. . . ],” ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users,” and open participative and consensus driven governance. This is in some ways a restatement of the WSIS principles and the basic premise of multi-stakeholderism. The outcome of the NetMundial process, hoped by some to be a Bolshevik-style contre-pointe response to evangelical proponents of multi-stakeholderism, not only largely conformed to existing multi-stakeholder catechism, but was coopted by the “mainstream.” Both ICANN and the World Economic Forum (WEF) adopted the mantel of implementing follow up actions from NetMundial including promoting “human rights and shared values.” This human rights theme will occur again in the upcoming discussion of reforms affecting ICANN. A month before the NetMundial conference issued its pabulum findings, the NTIA announced a process to consider relinquishing its oversight over some technical functions performed by IANA to the multi-stakeholder community – in shorthand, the IANA transition. IANA, effectively a subsidiary of ICANN, traditionally performed certain technical functions essential for the smooth and secure running of the Internet. As mentioned above, these include control of the Internet Protocol addressing system (i.e., numbering resources, including IPv4 and IPv6), managing IP protocols, and managing the rootzone database for domain names (domain name management). NTIA has had oversight over these functions via a series of agreements with ICANN in 1998 under a Memorandum of Understanding (MoU). The MoU went through several iterations and morphed into what was then called the Joint Project Agreement (JPA), which itself underwent one amendment. In 2009, the JPA was replaced with a document called the Affirmation of Commitments. Over time, in each iteration of the agreement between NTIA and ICANN, NTIA has loosened its oversight over the performance of these IANA functions by ICANN. Consequently, this latest move by NTIA can be seen as part of a continuous evolution away from NTIA’s control and oversight over the IANA functions. The IANA transition process is just that – a process, albeit a process that is conditioned on satisfying NTIA that there will be a suitable arrangement in place to ensure that the multi-stakeholder community will take over NTIA’s role. That said, the process is scheduled for completion by September 2015. This process consists largely of various consultations and reviews. The first is a “community outreach,” followed by a “community dialogue input” to a steering group (SG) that has been established by ICANN, which is itself supposed to be multi-stakeholder in character. The SG will produce a proposal for the transition that will be subject to a public comment period. These comments will be reviewed by the SG and then to the ICANN board and finally to NTIA for approval. The take away is this: nothing has changed – yet. But the dynamics this year have unleashed forces further entrenching already polarized positions on essential matters of Internet governance. Mr. Snowden’s revelations fanned the flames of those promoting a multilateral, state-centric approach to Internet governance, confirming suspicions about Western power and multi-stakeholderism, but ultimately failed to shift Internet governance toward a new model. The IANA transition has been a long time coming and will only shift technical functions to new organizations, but within the current Internet governance model. Thus, the durability of multi-stakeholderism persists – for now.

David Satola and Michael J. Kelly are co-chairs of the Internet Governance Task Force, Cyberspace Law Committee, ABA Business Law Section.

**ADDITIONAL RESOURCES**

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

**Business Law Today**

**Guidance from ARIN on Legal Aspects of the Transfer of Internet Protocol Numbers**

By Ben Edelman, Stephen M. Ryan
May 2013
Bitcoin is a so-called “cryptocurrency” that can be used as a medium of exchange to make payments and facilitate consumer and business transactions – primarily over the Internet. It has garnered a lot of attention among technocrats and has also been written about extensively in the popular press. While its user base is still quite small compared to that of checks, credit and debit cards, and electronic funds transfers, a growing number of businesses are adopting bitcoin as a payment option for those customers who wish to use it. Nationally known merchants such as Dell, Expedia, and Overstock.com have jumped on the bitcoin band wagon, along with a number of smaller companies such as the New Mexico Tea Company and Grass Hill Alpacas. Even the United Way now accepts donations in bitcoin.

This article examines the legal risks and issues that a business should evaluate before accepting bitcoin as a form of payment. It provides a brief overview of bitcoin, addresses potential registration and licensing issues, and examines the tax implications of accepting the virtual currency. This article also discusses the use of bitcoin merchant service providers (BMPs), which act as intermediaries between a business and a customer wishing to pay in bitcoin. The BMPs provide a range of services including accepting bitcoin and paying the merchant in dollars, removing many of the barriers to accepting this new payment mechanism.

A Quick Overview of Bitcoin

Bitcoin is an Internet-based virtual currency which can be used to transfer value between parties. It is often classified as a “cryptocurrency” because it relies on cryptography to authenticate transactions. A bitcoin has no physical presence and no central authority administers the currency. It is not backed by any government and is not legal tender in any jurisdiction. It is not issued by or redeemable at any financial institution. A bitcoin only has value because other participants in the ecosystem ascribe value to it. The authenticity of any particular bitcoin may be verified by consulting a master database of bitcoins (called the “block chain”) which is maintained over a peer-to-peer network on the Internet. The entities which provide the hardware and software to host the database and authenticate transactions are called “miners” and they are periodically rewarded for their public service by being given a few bitcoins. This is how new units of the virtual currency come into existence.

Bitcoin users are identified by their “public key” which is essentially a very large number. The public key is cryptographically associated with another large number, the “private key” which the user keeps confidential and uses to mathematically sign transactions. Because keeping track of these large numbers can be cumbersome, users typically employ a special piece of software called a “wallet” to manage their public and private keys. That software may be located on a personal computer or smartphone or hosted in the cloud by a service provider. While bitcoin is sometimes described as an anonymous currency, every transaction is recorded in the publicly accessible block chain and is associated with a public key. Tying a particular public key to an individual or company may be difficult, but it can be done. Bitcoin users, and merchants in particular, should assume that their bitcoin transactions are public knowledge.

To make a payment, a person uses his or her cryptographic credentials to sign a transaction transferring some amount of bitcoin to another person and submits it to the block chain. The miners perform
the mathematic calculations necessary to verify the transaction, and if it is deemed authentic, update the block chain to indicate the transfer of ownership. The whole process takes a couple of minutes maximum. Once written to the block chain, the transaction is not reversible.

The price of a bitcoin relative to the U.S. dollar has fluctuated dramatically over time. In the early days of the virtual currency, it was worth on a few cents. As its fame increased and speculators began to invest, the price increased dramatically, reaching a high of $1,162 on November 30, 2013. The exchange rate has since retreated from that peak, falling to around $300 in early October 2014. Volatility is likely to be an aspect of the bitcoin market for the foreseeable future and consequently should be a consideration for businesses which engage in transactions denominated in bitcoin.

**Licensing and Registration Requirements for Bitcoin Related Businesses**

At both the federal and state levels, there are requirements that entities engaged in certain financial service activities register or obtain a license if they wish to operate within the jurisdiction. While the boundaries of these laws are not always as sharply delineated as business lawyers might like, it seems reasonably clear at this point in time that a business which merely accepts bitcoin as a payment mechanism on its own behalf has no obligation to register or obtain a license. As is discussed below, however, the law in this area is in a state of flux and merchants accepting bitcoin are advised to stay current with developments which may affect them.

At the federal level, the Bank Secrecy Act (BSA) requires an entity which issues traveler’s checks or money orders, performs check cashing, engages in money transmission, or provides certain other services to register as a Money Services Business (MSB). Along with the duty to register, an MSB is obligated to develop an anti-money laundering plan, keep certain records, and report certain transactions and other suspicious activity to the government. The Financial Crimes Enforcement Network (FinCEN), the agency which administers the BSA, has issued guidance explaining when a bitcoin business might be deemed to be engaging in money transmission and thus be obligated to register.

For BSA purposes, money transmission is defined as the acceptance of currency or other value that substitutes for currency from one person, and the transmission of that currency or substitute to another location or another person by any means. Currency is defined to mean the legal tender of the United States or another country. Under these definitions, bitcoin is not a currency, but it is something that can substitute for currency, and thus its acceptance and transfer to another person or location would constitute money transmission. In its guidance, however, FinCEN makes clear that when a person obtains bitcoin and uses it to purchase goods or services, there is no acceptance from and no transfer to another person. Consequently, a person or business that uses bitcoin solely for its own purposes and not for the benefit of another is not an MSB. While FinCEN’s guidance does not directly address the merchant scenario, it seems clear that a business may accept bitcoin in exchange for goods or services and not be obligated to register. Furthermore, the business may hold on to that bitcoin, exchange it for dollars, or even use it to pay a vendor and not trigger the rule. A merchant that is careful to limit its use of bitcoin to its own purposes and does not provide bitcoin services to others should have no obligations under the FinCEN rules.

At the state level, many jurisdictions also require entities engaged in money transmission to obtain a license and to meet certain requirements for safety and soundness, as well as consumer protection. While the concept of money transmission at the state level is similar to that expressed in FinCEN’s rules, there are differences between state and federal law, and indeed, a fair amount of variance among the state statutes. A few states have opined on the application of their money transmitter laws to bitcoin related businesses. In April of 2014, Texas regulators confirmed that bitcoin does not constitute “money” or “monetary value” as defined in their Money Services Act, and thus bitcoin transactions are not covered by the law. These regulators did acknowledge, however, that bitcoin related businesses such as wallet providers, currency exchanges, and ATM operators which receive government-issued currency for certain purposes might still be covered.

In contrast, the North Carolina Commissioner of Banks has stated that bitcoin does constitute “monetary value,” and thus activities involving the cryptocurrency may be covered by the state’s money transmitter law. The agency indicated that it is working on new regulations to address when virtual currency users are engaged in money transmission and noted that changes to the underlying statute may be necessary in order to keep up with the market place. New York has taken a different approach, proposing a regulatory scheme just for virtual currencies. On July 17, 2014, the New York Department of Financial Services issued a draft version of its “bitlicense” regulations for public comment. The rules would cover entities engaged in “Virtual Currency Business Activity” which includes receiving, storing, and transmitting virtual currency. The rule, however, would not cover merchants accepting bitcoin in consumer transactions.

It seems reasonable at this stage to conclude that a merchant that accepts bitcoin or other virtual currencies for its own account in order to facilitate the sale of goods and services will not need to be licensed or register with any governmental entity. The merchant should be careful, however, not to provide bitcoin related services such as transfer or exchange to its customers. And finally, because this body of law will continue to grow and change, the prudent business will actively monitor regulatory developments in this area.

**Tax Implications of Accepting Bitcoin**

When a business or individual conducts a transaction in a foreign currency, there are special rules which govern how gains or
losses from the exchange of foreign currency are handled for tax purposes. Many bitcoin users assume that those rules would also apply to virtual currencies. Such hopes were dashed by IRS guidance issued in March 2014 which concludes that, for federal tax purposes, bitcoin and other virtual currencies should be treated as property and not foreign currency. This interpretation by the IRS has enormous business implications for merchants accepting bitcoin and has been criticized by commentators.

The IRS explains that for tax purposes virtual currency should be treated as property and that general tax principles which apply to property transactions will govern the tax treatment of bitcoin. When acquiring property, one is required to record the fair market value of the property which is deemed the owner’s “basis” in the property. When the asset is later exchanged, if the fair market value has increased, then the owner has a taxable gain. If the sale price is less than the taxpayer’s basis, he or she has a loss. Applied to virtual currency, this means if a person accepts a bitcoin on Monday when the value is $400 and then makes a purchase with that same bitcoin on Friday when the value is $410, he or she has a $10 gain. Imagine a merchant that acquires bitcoin in multiple transactions over a month during which the price of bitcoin fluctuates. Its basis in each individual bitcoin may be different depending on the market price at the time of the transaction. When the merchant decides to cash out some of its bitcoin for dollars, it will need to decide not just how much bitcoin to sell but also which particular bitcoins to part with – because exchanging this bitcoin over that bitcoin will determine the amount of a reportable gain or loss. Needless to say, the amount of record-keeping necessary to track the basis in each bitcoin and compute gains and losses makes it impractical for many businesses to accept bitcoin. One work-around for this problem is for a merchant to exchange bitcoins for dollars immediately upon acceptance before the fair market value of the asset can change. An automated procedure to handle these exchanges would simplify but not eliminate the merchant’s record-keeping obligations, although creating such a process would involve a significant investment in time and resources. Lucky for merchants, third-party service providers exist to offer just this type of service.

Using a Bitcoin Merchant Service Provider

In response to the tax accounting and record-keeping issues described above and other legal and operational problems facing merchants which wish to accept bitcoin, a new category of service provider has emerged – the BMSP. Coinbase and BitPay are probably the best known of this class of vendors, but a quick Internet search reveals a growing number of players in this space. The BMSP essentially acts as an intermediary, accepting bitcoin from the customer and providing dollars or some other currency to the merchant.

In a typical implementation, the merchant adds a button to the checkout page of its website labelled “pay with bitcoin.” If the customer chooses this option, he or she then interacts with the BMSP’s servers to provide information necessary to pay using bitcoin. The BMSP initiates the bitcoin transfer and notifies the merchant when the bitcoin transaction is complete. The merchant then completes the purchase transaction with the customer and ships the goods. The BMSP settles with the merchant on a prearranged schedule, usually daily, by electronically transferring dollars or euros or some other supported currency to a bank account designated by the merchant. Some BMSPs also support settling in bitcoin or other virtual currencies. While pricing varies, several providers offer plans with no transaction fees.

An obvious benefit of using a BMSP is that a merchant can enable its customers to pay with bitcoin without ever actually having to receive or hold bitcoin itself. Such an arrangement would reduce or eliminate the accounting and record-keeping obligations associated with the IRS guidance, making virtual currency acceptance a significantly easier and more attractive option. Introducing an intermediary into the relationship with a customer, however, brings new risks which require careful evaluation. Before engaging a BMSP, a merchant might want to ask the following questions:

1. **Is the BMSP a registered MSB?** A BMSP accepts bitcoin from a consumer and provides dollars to the merchant. This action clearly constitutes money transmission under the BSA as discussed above. Merchants should confirm their BMSP is properly registered and in compliance with FinCEN regulations. Ask the provider for a copy of its written anti-money laundering compliance program. If it doesn’t have one, it’s not in compliance.

2. **Is the BMSP a licensed money transmitter in the appropriate states?** While there is more variance and uncertainty in state law, it seems likely that a BMSP would also be deemed to be a money transmitter in at least some states. A prudent merchant will determine if the BMSP is licensed in the jurisdiction in which the merchant operates, and if not, why not.

3. **What is the settlement risk in using a BMSP and how can it be mitigated?** There will be a delay of several days or more between the time the BMSP accepts your customer’s bitcoin and the time you get paid. There is always a risk that the BMSP won’t settle on time or at all. Merchants should evaluate and understand this risk before engaging a BMSP. Settling more frequently will reduce the risk of nonpayment. In addition, a licensed money transmitter will be required to post a bond or pledge collateral to ensure its ability to make good on its obligations to its customers. Consequently, licensure reduces settlement risk.

4. **Are there sufficient disclosures explaining the transaction and the role of the BMSP?** Is the consumer given sufficient information to understand the transaction and the fact that he or she is paying the BMSP and not the merchant? Does the consumer understand that by paying with bitcoin, he or she will not have the consumer protections associated with credit and debit card payments? Merchants should review the Consumer Financial Protection Bureau’s advisory to consumers using virtual currency and ensure that
their disclosures appropriately address the agency’s concerns.

5. How is the exchange rate determined and disclosed? How is the exchange rate being applied to the customer’s bitcoin transaction being calculated? How is it disclosed to the consumer? Is the rate fair and competitive? Especially in situations where the BMSP is not charging the merchant a fee, there may be concern that the exchange rate will be padded in order to generate additional revenue.

6. How will the merchant handle refunds? Typically, merchants make customer refunds using the same payment method employed in the original transaction. While some BMSP offer the ability to make refunds in bitcoin, that process may not be convenient. If a refund is made in bitcoin, will you refund the dollar amount or the bitcoin amount of the original transaction? Are your policies in compliance with the Federal Trade Commission’s recently updated Mail, Internet, or Telephone Order Merchandise Rules requiring refunds be made either in the method used by the buyer or by cash, check, or money order? Is the refund policy as it applies to bitcoin transaction properly disclosed to the customer?

7. What privacy protections govern the bitcoin transaction? What information about your customer are you providing to the BMSP? What are the BMSP’s practices regarding the collection and disclosure of personal information about your customer? Are the BMSP’s privacy practices adequately disclosed? Do the BMSP’s privacy policies mesh with your own?

Conclusion
Given the increasing interest in bitcoin among the public, merchants understandably want to be able to accept it as a form of payment. Managing the legal and tax implications associated with virtual currencies is a new challenge which business lawyers must address. The use of a properly managed BMSP can simplify the operational issues and reduce the legal risks of accepting bitcoin.

Stephen T. Middlebrook is general counsel at FSV Payment Systems, Inc. He serves as co-chair of the Electronic Payments Subcommittee of the Cyberspace Law Committee, ABA Business Law Section. He is also the Section’s advisor to the Uniform Law Commission’s Study Committee on Alternative and Mobile Payments. The opinions expressed in this article are those of the author and do not necessarily reflect the views of his employer or any other entity.
Net Gets Physical: What You Need to Know About the Internet of Things

By John A. Rothchild

The Internet of Things (IoT) has become a hot topic in venues as disparate as consumer electronics shows and government regulatory proceedings. The topic is a big one, and is poised to get much bigger. This article will introduce the IoT and address some of the legal issues that will accompany its growth.

There is no universally accepted definition of the term “Internet of Things.” It is generally used to refer to the collection of physical objects that are linked to each other, and to users, through the Internet or other computer networks. Since computers themselves are not usually thought of as belonging to the IoT, it might be more accurate to limit the scope of the IoT to the, still-fuzzy, “things that didn’t used to be connected to the Internet, but now are.” Examples of objects that belong to the IoT include:

• A home security system that can be monitored and controlled via the Internet
• A sensor in your basement that sends you a message when it detects flooding
• An oven that can be controlled using your smartphone
• A bathroom scale that sends your weight readings via the network to your doctor
• Implanted medical devices, like pacemakers and insulin pumps, that can be controlled wirelessly
• Wearable devices that count the number of steps you take and display the information on a website
• A dog collar that lets you geolocate your pet
• Smart electrical metering systems that transmit your usage information to the utility
• Home thermostats can be controlled via a mobile device and that compile and display your usage
• Automobiles with telematics systems that allow them to be monitored and controlled remotely
• RFID tags attached to pallets holding a vendor’s inventory
• Sensors on jet engines that relay performance information to a monitoring system

There have long been non-computer “things” connected to the Internet. Technology archaeologists trace the IoT back to a Coca-Cola vending machine at the Carnegie Mellon University Computer Science Department. In 1982, grad students wired it up to the university’s network so that users of the machine could check from their desks whether it was empty and whether the bottles were cold. Commercial and industrial applications have also been common for some time. For example, in 2005, Wal-Mart began mandating that its suppliers place RFID tags on shipping pallets to facilitate inventory control. But the IoT has burst into popular consciousness only in the past year or two. At the Consumer Electronics Show in January 2014, IoT devices got what one report called “the lion’s share of the spotlight,” featuring, among many other curiosities, a connected toothbrush. In the same month Google announced that it would purchase Nest Labs, maker of the eponymous Internet-connected home thermostat, for a stunning $3.2 billion. In November 2013, the Federal Trade Commission (FTC) picked up on the trend with a day-long workshop titled “Internet of Things: Privacy and Security in a Connected World.”

If projections are anywhere near accurate, the IoT is going to get much, much bigger. In December 2013, the technology research firm Gartner predicted that the number of IoT devices will grow to 26 billion in 2020 (from 900 million in 2009), with associated revenues exceeding $300 billion – far outstripping the predicted 7.3 billion personal computers, tablets,
smartphones. Market research firm IDC says the market of goods and services surrounding the IoT will reach an astounding $8.9 trillion in 2020, which is about the current GDP of China.

The omnipresent IoT will give rise to a whole range of legal issues. The following discussion will address two of them: (1) privacy and security, and (2) remote disablement of connected devices.

Privacy and Security

Privacy and security issues are inevitable, arising from the facts that (1) objects on the IoT transmit information via public data networks, (2) the information these objects gather is often transmitted to third parties, (3) users of the devices are often unaware of how their information is used by those recipients, (4) privacy and security considerations have not been of central concern in the design of IoT devices, and (5) some IoT devices are designed to spy on users.

1. Transmission of sensitive data via public networks. In many applications, data collected by IoT devices travels from the device via a wired (HomePlug) or wireless (Wi-Fi, Bluetooth, near-field communication, radio-frequency identification) connection to the Internet, which then routes the information to its intended recipient. The Internet is not an inherently secure medium for the transmission of information, and becomes secure only with the addition of encryption-based systems to prevent unauthorized access. But connected IoT devices do not always incorporate adequate security.

An example of such a lapse occurred with a wireless camera system sold by a company called TRENDnet, Inc. The cameras, designed for use in homes and small businesses and (ironically as it turned out) sold under the SecurView brand name, connected to the Internet via Wi-Fi wireless networking. The system was designed so that the camera user could monitor the live video and audio feeds via the Internet. According to the FTC, a flaw in the camera’s software allowed a hacker to discover IP addresses that allowed the feeds to be monitored. The hacker posted this information online, allowing anyone to monitor feeds from nearly 700 of the cameras. The FTC noted that “these compromised live feeds displayed private areas of users’ homes and allowed the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities. The breach was widely reported in news articles online, many of which featured photos taken from the compromised live feeds or hyperlinks to access such feeds.” The order settling the case requires TRENDnet to establish and maintain “a comprehensive security program.” In re TRENDnet, Inc., FTC Docket No. C-4426 (2014) (consent order). In its press release, the FTC described the case as “the agency’s first action against a marketer of an everyday product with interconnectivity to the Internet and other mobile devices – commonly referred to as the ‘Internet of Things.’” It will not be the last.

2. Transmission of sensitive data to third parties. Privacy risks also arise from the fact that data collected by IoT devices is often routed to third parties. For example, the energy usage of a household that has a smart metering system is collected by the utility. Patterns of electricity usage are surprisingly revealing of the activities that give rise to that usage. Law enforcement agencies have for some time made use of household monthly electricity bills to identify houses in which marijuana plants are being grown; the grow lights consume lots of electricity. Much more detailed information about household activities can be derived from the usage patterns collected by smart meters. Usage profiles can be mined to determine at what times a washing machine, a toaster, or a kettle is operated. According to a report from NIST, data collected from a residential smart electricity meter can reveal when the occupants sleep, eat, shower, and watch television; the residents’ work schedule, sleeping patterns, and other lifestyle habits; how many people are living at the house; whether anybody is home; and where they are located in the house. Revealing data may also be collected via plug-in electric vehicle charging stations, including the location of the vehicle each time it is charged. Information of this sort may be of interest to insurance companies, marketers, law enforcement authorities, private litigants, landlords, creditors, the press, and criminals. See National Institute of Standards and Technology, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid (2010). Plans to network smart appliances via home area networks will provide utilities (and, in principle, consumers) with still more detailed information about home electricity usage.

Data from use of electrical appliances may also be routed through the appliance manufacturer. A representative of General Electric explained at the 2013 FTC hearing that the data it collects from connected residential ovens and other electrical appliances is currently not exploited, but in the future, GE may decide to use it for marketing purposes.

There is presently little effective legal protection of the privacy of data collected via the smart grid. State legislators have begun to take notice. In 2010, California enacted the first state law specifically protecting smart grid data. The statute provides that, with certain exceptions, “[a]n electrical corporation or gas corporation shall not share, disclose, or otherwise make accessible to any third party a customer’s electrical or gas consumption data.” Cal. Pub. Util. Code § 8380(b)(1). While various general purpose state and federal privacy laws may in theory protect the privacy of data collected via the smart grid, a 2011 article concluded that existing privacy protections are inadequate. See Cheryl Dancey Balough, Privacy Implications of Smart Meters, 86 Chi.-Kent L. Rev. 161 (2011).

3. Users’ lack of awareness. These privacy and security issues are exacerbated by the fact that most users of IoT devices have very little understanding of the data flows associated with their usage and their potential impacts. Consumers are not accustomed to the idea that the everyday devices with which they interact, and which formerly were their mute and obedient servants, may now be sharing their personal information with unknown third parties. Her refrigerator may be blabbing...
to Electrolux (the Swedish manufacturer that in September 2014 purchased General Electric’s appliances division), her thermostat may be whispering to Google (the new owner of the Nest connected home thermostat). Her Fitbit is definitely collecting information about her movements and sending it to Fitbit, Inc.’s computer servers. Fitbit’s privacy policy, available from its website, states that it does not share personally identifiable information with third parties except in narrow circumstances. But it also advises that “this policy may change over time. If any modifications substantially change your rights under this policy, we will send you an email where possible, and always provide notice on the Site.” How many Fitbit users will ever consult the manufacturer’s website to assess the privacy implications of wearing that activity tracking device? This points to a key privacy issue with IoT devices: typically those devices will lack a user interface that makes it feasible to deliver notice to the consumer about the privacy implications of her use of the device.

The manufacturers of IoT devices are apparently not trying very hard to inform consumers of the uses that are made of personally information collected via these devices. A study of health and fitness smartphone and tablet apps by a privacy advocacy group found that:

- 26% of the free apps and 40% of the paid apps had no privacy policy
- Only 43% of free apps and 25% of the paid apps provided a link from within the app to a privacy policy on the developer’s website
- 39% of the free apps and 30% of the paid apps sent data to someone not disclosed by the developer
- Only 13% of free apps and 10% of paid apps encrypted all data transmissions


4. Manufacturers’ lack of incentives. The tendency of IoT devices to lack effective privacy and security features is due in large part to the absence of any perceived incentive to expend resources on such features. Manufacturers believe, perhaps with justification, that they will get little return on their investment in such improvements. As a speaker at the FTC’s 2013 hearings noted: “There is no financial incentive to companies to make their devices secure. When is the last time you saw a bad review on Amazon because some product had a security vulnerability? Never.”

Researchers have demonstrated the vulnerability of certain IoT devices to unauthorized access and control, including implantable medical devices and automobiles. Some implantable medical devices are designed so that they can be controlled using a wireless connection to a device outside the body. Naturally, only medical personnel and the patient should be able to exercise such control. But a 2008 study demonstrated that a particular implantable pacemaker/defibrillator could be taken over and controlled by an unauthorized attacker. A simulated attack succeeded in determining what type of device was implanted, intercepting telemetry data from the device, changing the device settings, and delivering an electrical shock. Other studies have demonstrated the vulnerability of automobiles equipped with telematics systems. See Halperin et al., Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses (2008). A 2011 study showed that an automobile’s systems can be compromised through a variety of routes. One method required inserting a CD with special files on it into the car’s CD player. Another attack used a smartphone that connected to the car’s systems using Bluetooth, enabling it to deliver a Trojan horse application. A third attack was initiated by making a phone call to the car, which exploited a flaw and caused the car to download malicious code from the Internet. Since all of the car’s electronic systems are connected via the controller area network bus, once the car is compromised through any route, the attacker has access to all of the systems. The simulated attack was able to cause the car to Tweet the car’s GPS location, record conversations in the car’s cabin (using the microphone intended for hands-free phone operation), and command the car to unlock its doors on demand. See Checkoway, et al., Comprehensive Experimental Analyses of Automotive Attack Surfaces (2011).

5. Invasion of privacy by design. Some IoT devices have features that are designed to invade the user’s privacy. That was the case with software installed on rented laptop computers. Aaron’s, a national chain of rental outlets, installed PC Rental Agent software on computers that it rented to consumers. In addition to allowing the computer to be disabled remotely, the software collected personal information about the user. According to the FTC, the software had the capability of “logging keystrokes, capturing screenshots, and using the computer’s webcam,” and collected personal information such as passwords, medical information, bank statements, and photographs of the users in intimate situations. Aaron’s did not always disclose the presence of the software to the renter, or obtain her consent. Aaron’s settled an action that the FTC brought, agreeing to entry of an order prohibiting it from using monitoring technology on a rental computer. See In re Aaron’s, Inc., FTC Docket No. C-4442 (2014) (consent order).

Remote Disablement of IoT Devices

Another issue relating to the IoT that has not yet received much notice is the remote disablement of IoT devices by the vendor. Unlike ordinary consumer devices, which once sold are beyond the control of the device’s seller or manufacturer, an IoT device may remain accessible via the network. This allows the vendor to interact with the device so as to modify its functioning.

A well-publicized instance of this occurred in 2009, when Amazon.com remotely deleted two e-books, George Orwell’s 1984 and Animal Farm, from the Kindle e-book readers of consumers who had purchased the books. Amazon justified the deletions on the ground that it had discovered that the company that pro-
vided the texts of the books did not have rights to them; deleting the books would un-do Amazon’s unauthorized distribution of the texts. Amazon gave refunds to the affected consumers, but this did not prevent it from receiving a hail of criticism. A lawsuit against Amazon brought by a 17-year-old high school student in Michigan resulted in a settlement under which Amazon agreed not to engage in such conduct again.

A manufacturer or retailer may have various reasons for building in the capacity to disable a device remotely. Prominent among these is to retain the ability to put pressure on a buyer who purchases the device on credit and fails to make a required payment. Disabling the device, or threatening to do so unless payment is made, is an alternative to physical repossession of the device that offers substantial advantages to the creditor.

This practice has its antecedents in remote disablement of computers when the vendor believed that the owner owed money on the hardware or software. One method of accomplishing this is by including programming, called a “logic bomb” or “time bomb,” which causes the computer to stop functioning on a certain date if the user fails to enter a code that the vendor will only supply once the user makes the payment that the vendor demands. Several courts held this procedure to be improper. See, e.g., Werner, Zaroff, Slotnick, Stern & Askenazy v. Lewis, 155 Misc. 2d 558, 588 N.Y.S.2d 960 (N.Y. Civ.Ct. 1992) (breach of contract); Clayton X-Ray Co. v. Professional Systems Corp., 812 S.W.2d 565 (Mo. Ct. App.1991) (breach of warranty and conversion). A logic bomb that destroys computer data may also constitute a computer crime. See State v. Corcoran, 522 N.W.2d 226, 186 Wis.2d 616 (Wis. Ct. App.1994). However, software deactivation pursuant to the terms of a lease or sale may be justified. See American Computer Trust Leasing v. Jack Farrell Implement Co., 763 F.Supp. 1473 (D. Minn. 1991), aff’d and remanded sub nom. American Computer Trust Leasing v. Boerboom Int’l, Inc., 967 F.2d 1208 (8th Cir.1992).

An increasingly common use of remote disablement is in connection with automobiles that are purchased on credit. The vendor equips the car with a piece of equipment called a starter interrupt device. If the borrower fails to make a payment, the lender can send a signal to the device using his or her computer or smartphone, disabling the car’s ignition system. The device is typically used on cars that are sold on credit to borrowers with low credit scores. According to one report, the devices are used in about 25 percent of purchases that are financed with subprime auto loans. Starter interrupt devices replace the repo man with a system that is much more efficient. The devices incorporate GPS technology, so the lender can track the car’s location in real time. This allows the lender to shut down the car at a time that will minimize harm to the borrower, and potential damage to the car, such as by waiting until the car is sitting on the borrower’s driveway. The resulting intrusion on the borrower’s privacy is readily apparent. Some borrowers claim that their cars have been shut down while driving on a freeway or idling at a stop light, but manufacturers of the devices say that they are designed so this cannot occur. See Michael Corkery & Jessica Silver-Greenberg, Miss a Payment? Good Luck Moving That Car, N.Y. Times (Sept. 25, 2014), at A1.

The legality of using remote disablement to enforce a creditor’s rights is in many situations unclear. If the device in question secures a loan, Article 9 of the Uniform Commercial Code may apply. UCC § 9-609 limits the right of a secured party to exercise self-help in case of default, allowing equipment to be rendered unusable without judicial process only if it can be done “without breach of the peace.” This limitation would apply if a creditor sought to enforce a security interest in a business computer by disabling it via the network. The UCC does not define “breach of the peace” and the courts have not developed any uniform interpretation, so its applicability to remote disablement is unclear. However, the absence of physical confrontation makes a breach of the peace less likely with remote disablement than with sending out of the traditional repo man.

Several state enactments of § 9-609 impose additional limitations on this sort of electronic self-help. See Conn. Gen. Stat. Ann. § 42a-9-609(d)(2) (providing that electronic self-help is permitted only if the debtor has separately agreed to it, and the creditor gives 15-days’ notice before exercising self-help); Colo. Rev. Stat. Ann. § 4-9-609(e) (providing that the secured party may not disable a computer program embedded in the collateral “if immediate injury to any person or property is a reasonably foreseeable consequence of such action”).

The use of remote disablement in connection with consumer transactions is less clear. Section 9-609 does not govern the disablement of consumer goods, such as an automobile for personal use. The Uniform Computer Information Transactions Act (2000) (UCITA) prohibits use of electronic self-help as a remedy in case of breach of a license agreement in a consumer transaction. See UCITA § 816 (prohibiting use of “electronic self-help” in “mass-market transactions”). UCITA has been enacted only in Virginia and Maryland. The ALI Principles of the Law of Software Contracts (2010) (“ALI Principles”) forbid use of electronic measures as a remedy for contract breach in consumer transactions. See ALI Principles § 4.03 (forbidding use of “automated disablement” in consumer transactions). The ALI Principles are not law, but only a statement of recommended best practices.

There is little law that directly addresses the use of starter interrupt devices. In 2012, the California legislature enacted a law specifically governing the use of such devices by automobile dealers who provide their own financing and retain a security interest in the vehicle; such dealers often sell used cars to buyers with poor credit histories. The provision allows use of the devices as long as the seller notifies the buyer of the existence of the device at the time of sale, and provides 48-hours warning before using it. See Cal. Civ. Code § 2983.37. Many states have laws that regulate repossession of consumer goods, but it is unclear whether remote disable-
ment of a vehicle, which does not entail any loss of possession, would qualify as repossession under these statutes. Regulators in several states have issued informal opinions concluding that the use of starter interrupt devices is unlawful. For example, a 2012 opinion letter from the Wisconsin Department of Financial Institutions states that the use of starter interrupt devices “is prohibited” on the ground that it constitutes an unfair collection practice and is unconscionable.

**Conclusion**

Given the huge interest and investments that anything relating to the IoT is drawing, and with an anticipated installed base of billions of IoT devices in the coming years, lawyers, companies, and regulators are well advised to keep a close eye on this technological space.

*John A. Rothchild is an associate professor at Wayne State University Law School.*
The Practical Tech Lawyer: Advising a Company on Data Security Compliance

By Theodore F. Claypoole

JPMorgan Chase, Target, Home Depot, Lockheed Martin, the University of Hawaii, the States of Texas and South Carolina, TJX, Cedars-Sinai Medical Center, BNY Mellon, eBay, the U.S. military, T-Mobile, Sony. These are the type of clients that nearly all business lawyers would covet and fight to protect, and each has recently suffered a large and embarrassing data breach, likely to cost millions. How do you keep your clients off of this list? What will you say when your clients ask for your help in protecting their prized information?

Information security is a relatively new problem for many businesses. Over the past 20 years and accelerating over the past five, new burdens, technologies, enemies, and interested parties have forced businesses to invest larger budgets and more personnel toward protecting their data. These companies will ask their business lawyers to help to comply with the companies’ legal, regulatory, payment system, and contractual obligations. Some of the compliance complexity is based in technology, and therefore is outside of a lawyer’s reasonable realm of expertise. But much of the problem is structural, policy-based risk management which an attorney can and should manage.

This article will help you understand the broad strokes of danger, complication, risk, and protection for data security in business, health, educational, or governmental entities. Breaking the topic into discrete and practical viewpoints, the article can help the business lawyer better advise clients and minimize risks.

The Client

We start with an exploration of which entities should be committing significant resources to data security. All businesses, governments, and schools should be concerned that a serious cyberattack could shut down their operations. The more dependent a business is on databases or networked machines to perform its functions, the more vulnerable it is to cyberwarfare or other malicious attacks. Every modern business should have crisis management and disaster recovery plans to minimize these risks.

However, while acknowledging this problem, this article is primarily concerned with data protection, not with business stoppage. Any entity with customers, employees, benefit plans, patients, students, constituents, valuable research, or trade secrets must protect its data. One of the most important drivers of data protection has been the rise of identity theft, where a criminal assumes the financial, tax, health insurance, or immigration identity of an innocent person. Laws and regulations have arisen from the desire to limit identity theft. Therefore, any company holding identity-establishing information for individuals (known as “Personally Identifiable Data” or “PII”) must take steps to protect this information.

And this is especially true for financial data. Entities that take, hold, or process payment and financial account data are held to an especially high standard. Retailers, hospitals, colleges, personal or home service providers (like lawyers), and state licensing agencies all accept direct payments and will be responsible for protecting this data from exposure and loss. Banks and other financial institutions hold the mother lode of personal data, as well as holding people’s money itself (primarily in digital form), so they are tightly regulated in their use and protection of this information.

Health-care data, children’s information, student records, and video rental information are also specially regulated and protected under U.S. law, so companies that hold this data must meet the requirements of regulators. Nearly every U.S. state and territory has a law regulating treatment of consumer data and imposing obligations upon businesses who expose such data, so that anyone regularly interacting with consumers should be aware of the applicable
laws and what these laws require. States interpret these laws to protect the data of their residents, so the residency of the affected consumer will determine which laws apply, not the location of the business exposing the data.

Any business with employees has obligations on how to treat sensitive information about them. Employee health information or benefit plan data can fall within the health-care data protection laws. Businesses without a consumer contact may still be required to implement data security systems to protect their employee information.

Finally, many companies have secrets of their own. Trade secrets will only be protected under U.S. federal and state laws where the holder of those secrets takes steps to protect the secrets from exposure. In addition, some businesses hold technology and research of national importance to the defense and advancement of the nation. Companies like these should consider keeping such information completely off-line, where prying eyes half-way around the world could not reach them through electronic channels.

If a client falls into any of these categories, then the client should be considering how to protect the data it holds. As a lawyer, you can advise your client of the special risks and realities surrounding information management.

The Problem
Data security is a misunderstood term. Nothing in a business is entirely secure, and no one can guaranty absolute protection. In order for information to have value to a business, the company must be able to reach it and use it. If the company executives can reach the valuable information, then a motivated attacker can also reach it, even if the attacker cleverly disguises him or herself as the executive who is allowed access. Data security cannot be an exercise in hermetically sealing off data so that it can never be accessed. Instead, it is an exercise in making the data so hard to reach for unauthorized people that the unauthorized people find easier targets elsewhere, walking away frustrated and leaving your clients alone. A business is only secure relative to the sophistication of the threats against it and relative to other businesses.

Information security is also about resources. Since a business cannot spend all of its money trying to secure data (the business would bankrupt itself), and since no amount of money will absolutely secure a company’s data, the company must carefully allocate enough funds to data security and carefully choose the most efficient expenditures of those funds. A business can always be made more secure with more money and more manpower defending information, but like nearly all business expenses, data security spending creates diminishing returns. At a certain point, your dollar buys you less and less security than the early dollars purchased. For this reason, a lawyer’s best advice may protect data with cost-efficient but highly effective solutions like risk-reducing policies, practices, training, and organizational structure.

When your client is the victim of a successful cyberattack, the client is publically humiliated and treated no better than the criminal attacker. The business victim of a successful data theft suffers official fines and class action lawsuits. The U.S. Federal Trade Commission (FTC) has starkly argued that failure to protect consumer data is “an unfair and deceptive” act on behalf of a business, and state attorneys general have also sued to compensate the consumer victims of data theft. Banks and credit card companies nearly always fine a business for exposing card data.

Some of the reason for this harsh treatment of corporate and government attack victims arises from our society’s refusal to see the complexity and impossibility of absolute data protection. People need to feel that their data can be protected or they would lose faith in the entire system, so we heap abuse on the company unlucky enough to provoke a brilliant attack by a dedicated criminal, even where the attacker is as rich and sophisticated as the army of the People’s Republic of China. We assume that this business should be able to protect our information no matter what happens, so the fact that it did not protect our data is an obvious failure.

But some of the business blame arises from the fact that our legal system, referencing the underlying tenets of the Uniform Commercial Code, tends to allocate business risk to the party who dealt most closely with the wrongdoer. We know that if someone gets away with a theft of money in our commercial legal system, one of the innocent parties will be stuck with the loss, unless and until that thief may be brought to justice. The innocent parties in commercial banking transactions tend to be the account holder (consumer), the account holder’s bank, the person the account holder was paying, and the payee’s bank. Our system tends to protect the consumer, who has the least control over protection of the funds: if the money was stolen from the consumer’s account, we allocate the loss to the consumer’s bank; and if the money is stolen from the payee’s bank before it reaches the payee, that bank will be accountable. Similarly, we expect companies holding consumer information (and other valuable data) to be responsible for protecting it, and we penalize those companies for a data breach.

This system feels particularly unfair to a business held responsible for the loss, but this system of commercial blame is grounded in policy. Such a system encourages companies to take steps to protect data and avoid losses, and it encourages consumers to use the commercial systems that facilitate modern commerce.

The Complications
Protecting digitized information is infinitely complicated. As noted above, nothing valuable can ever be totally secure. In addition, the technology holding and protecting our data changes rapidly, so one method of securing the data cannot be relied up as a permanent solution. Important data was once kept on paper in filing cabinets. Next, we kept it in databases in mainframe computers accessed only from our offices. We spread the access out to Internet enabled devices, and eventually to handheld mobile devices. Now we store important data with contractors in the cloud. Each of these changes requires a shift in security methods, technology, and philosophy.
Furthermore, the threats keep changing as well. Attackers are constantly attempting new methods of breaking into data files. One of the lessons learned in Target’s data breach was that sophisticated tools for hacking into companies are invented by brilliant hackers and then sold to average criminals, who only have to be pointed to the target to create a devastating attack. This trend is the cyber-equivalent of providing top-of-the-line military tanks at a low cost to anyone who wants to physically break into a bank vault. Our protections grow more sophisticated, but so do the attackers. Companies constantly change defenses to stay ahead of the hackers, but the hackers are constantly evolving their own models as well.

Finally, a business can only pay for a certain amount of security, and so its data protection should be a factor of the amount and type of data it must protect with consideration of the amount it can spend on security. We would not expect a one-branch corner bank to build the same data security scheme as Wells Fargo or Bank of America. All are banks, but each has different security profile, and therefore different amounts spent on information protection. The big banks are likely to be aggressive and pay for monitoring services searching the hacker’s message boards for signs of an upcoming attack. The small bank can only afford to build a defensive perimeter and to encrypt its data. All companies can afford protective policies and procedures, but the more employees a company hires, the more expensive and complicated are its plans.

A bank would have a different security profile from a government entity or from a retailer, even if they are protecting the same amount of data. The kind of access and contact allowed to customers/stakeholders is another differentiator for how a company organizes its data defenses.

The Adversaries
When data was stored in physical filing cabinets, a thief would need to place him or herself at physical risk to take the information. Upon connecting all of our databases to the Internet, hackers could steal data from a distance. At first these hackers were talented amateurs, often students looking to test themselves or to find the thrill of solving a complicated puzzle. No more. The people attacking company files now are professional gangs connected to the highest levels of organized crime. Some are even sponsored and protected by state actors, like Russia and China. In addition, some nations, like China and France, use the full power of their governments to help national industries by taking secrets from U.S. companies and research labs.

A world of support functions has also grown up around the data theft industry to help those people who break into businesses. We talked about the democratization of hacking tools above. But there are also secondary markets, found on the Internet, where people who steal consumer information can sell that data to ready buyers. An entire industry of finding and using data has grown around the practice of hacking into businesses.

The Obligations
If a client asks its lawyer to build an appropriate data security regime, the lawyer’s first step should be to examine the client’s specific data protection obligations. For example, hospitals, pharmacies, and doctor offices in the United States are regulated by the Health Insurance Portability and Accountability Act (HIPAA), which describes what patient care data must be protected. HIPAA includes a data security rule which provides instructions for certain required protective actions. Similarly, any financial company (Gramm-Leach-Bliley and FFIEC regulations) or school (FERPA) must follow a set of legal regulations written for one kind of data.

The FTC acts as data protection regulator for those businesses that do not fall under another set of regulations. The FTC requires companies to comply with their own privacy policies, website terms of use, end user license agreements, and other consumer contracts. State attorneys general enforce the data protection rules, like those in Massachusetts that require written information security policies.

Pursuant to its long-standing requirement that companies report material developments to investors, the Securities and Exchange Commission (SEC) has issued cyber-risk and security guidelines requiring public companies under its purview to better control and report on cyber-protection issues, and the SEC will hold a company’s board of directors responsible for lapses in information security. New audit guidelines from the SEC bring this requirement into focus for many businesses, and new fines are likely to follow.

Some of the most important data obligations are not written into U.S. law. If a business wants to accept credit or debit cards as payment it must comply with the Payment Card Industry Data Security Standards. This set of standards is required and enforced through a retailer’s contract with its merchant bank. Companies have been fined millions of dollars for failing to comply with these contractual standards, and the payment card industry holds out the threat of banning a business from the payment card system for repeated and egregious failure to follow these rules.

Many businesses are obligated to protect data through contracts with other companies. For example, a business that processes information for a regulated entity will be required by contract to comply with the data regulations that apply to its commercial customers. A company processing certain types of patient health data will be required to sign a business associate agreement that passes data protection obligations on to the processor. In addition, all types of businesses, regulated or not, protect their own data and have been aggressively applying similar standards to the companies that hold or process data for them.

Sometimes data obligations arise through the transfer of information across borders. For example, Canada and the European Union have legal schemes that are, in many ways, more protective of personal data than the laws of the United States. These jurisdictions limit the type of information that can be transferred to the United States, and limit the entities that can receive such data. Many U.S. companies with customers in foreign countries are subject to data obligations arising in those countries.

A lawyer should find all of the sources of sensitive and protectable data that his or
her client possesses, and examine all the obligations that apply to this data, whether those obligations arise from U.S. law or regulation, foreign law or regulation, contracts that are part of the payment system, or individual agreements with customers.

The Solutions

Once a client’s data obligations are identified and understood, then a lawyer should help his or her client devise security solutions to meet those data obligations. Many data protection rules provide road maps to compliance. For example, the Payment Card Industry Data Security Standards provides a framework for developing a security program around payment card data. The website for the Payments Card Industry Security Standard Counsel includes self-assessment questionnaires, specific requirements for PIN transaction security, and a list of validated applications that meet their standards. Its website also includes reference guides for merchants to learn how to be compliant with their rules.

The laws requiring information security have published audit guidelines to describe how the laws will be enforced. Federal Financial Institutions Examination Council (FFIEC) standards for the financial industry are created by a collection of the most important federal financial regulators, and address all aspects of data security in the financial services industry, from call center fraud to bank branch security. FFIEC publishes white papers describing the likely threats to financial data and how to address them, and it publishes direct security guidance to regulated entities and the audit handbook for making certain that regulated entities comply. Similarly, HIPAA audit standards are published by the U.S. Department of Health and Human Services (HHS). The HHS website includes protective documents on meeting the standards of the HIPAA Security Rule like “Security 101 for Covered Entities” and “Basics of Risk Analysis and Risk Management,” as well as specific data on physical safeguards, technical safeguards, and administrative safeguards. HHS also addresses the special needs of smaller providers who might not have the resources to implement all of these safeguards.

A lawyer can use these road maps and audit guidelines as baselines to develop data protection plans to meet the related obligations. It should be a necessary first step toward meeting data obligations that the lawyer and client analyze specific compliance material and guidance offered by the regulator or entity charged with enforcing certain data security obligations. Whether the PCI DSS, SEC, FFIEC, HHS, FCC, or FTC, these entities will give the most specific instructions on how to comply with relevant data security requirements. In addition, the U.S. government publishes its own set of standards for protecting data, published by the National Institute for Standards in Technology (NIST), especially its Computer Security Division. NIST provides useful protocols, sample security regimes, and white papers on important data protection practices. While often too detailed and expensive to be implemented in whole cloth by smaller companies, the NIST standards are a good place to learn how to think about data security, and to see how to protect vulnerable aspects of your client’s systems.

Some of the helpful NIST publications include guidelines for securing wireless local area networks, supply chain management practices, and how to use cryptographic key management systems.

A lawyer should remind clients that businesses are required to have sensible, logical, industry-standard solutions for data security and to seriously consider the protection of sensitive information. Companies will not be expected to have perfect security in all cases. A client must demonstrate the logic behind its data security plan, so some consultation with lawyers and technical specialists familiar with data protection will be important. A business can use this consultation to demonstrate that it built protection on solid industry standards. Equally as important is documenting the security regime and the reasons for making certain investments over others. Resource choices will be examined in an investigation following data loss, and well-considered choices can keep a business from suffering penalties or punitive damages upon losing customer information.

Attacks on client business will continue, and some will be successful. The lawyer’s job should be to prepare a client not only to fight these attacks, but to manage expectations and prove the logic of its plans when an incident turns into a data exposure. Lawyers are risk management professionals, and data security is an act of risk management. The attorney’s voice is valuable in building a protection plan that meets the client’s obligations, including preparation of the policies, procedures, and worker/executive training necessary to implement the plan, and documenting the decisions that underlie that plan.

Theodore F. Claypoole is a partner at Womble Carlyle Sandridge & Rice, LLP, in Charlotte, North Carolina.
On September 10, 2014, the Securities and Exchange Commission (SEC) announced charges against 28 officers, directors, and major stockholders of public companies for violating Section 16(a) and/or Section 13(d) of the Securities Exchange Act of 1934, as amended (the Exchange Act). These rules require prompt reporting about holdings and transactions in the stock of publicly traded companies. Six public companies were also sanctioned for contributing to filing failures by insiders or failing to report their insiders’ filing deficiencies. A total of 33 out of these 34 individuals and companies agreed to settle charges and pay financial penalties totaling $2.6 million. See “SEC Announces Charges Against Corporate Insiders for Violating Laws Requiring Prompt Reporting of Transactions and Holdings,” SEC Press Release No. 2014-190 (September 10, 2014), and “SEC Announces Fraud Charges Against Biotech Company and Former Executive Who Failed to Report Insider Stock Sales,” SEC Press Release No. 2014-191 (September 10, 2014).

SEC’s Strategy and Tools Prompt New Look at Issuers’ and Insiders’ Filing Obligations

These sweeping actions are another step in the SEC’s initiative to “fix broken windows,” as described by SEC Chair Mary Jo White in her public remarks on October 9, 2013. White explained the SEC’s efforts to ensure that its enforcement program is pursuing all types of violations of the federal securities laws, big and small, thus “casting its nets wider, and into smaller spaces, paying attention to violators and violations regardless of size.” See Mary Jo White, “Remarks at Securities Enforcement Forum 2013,” Washington D.C., Oct. 9, 2013. She noted that the SEC is streamlining its investigations, particularly those involving strict liability where there is no need to prove intent, such as in the case of Exchange Act Section 16(a) and Section 13(d) reporting violations. This is a noteworthy change in that these types of reporting violations, by themselves, traditionally have not been a source of significant SEC enforcement interest in the absence of other alleged violations or bad facts.

In announcing these charges, Andrew Ceresney, Director of the SEC’s Division of Enforcement, noted that the SEC brought these actions together to send a clear message about the importance of abiding by the reporting requirements of the federal securities laws. Ceresney issued a stern warning: “Officers, directors, major shareholders and issuers should all take note: inadvertence is no defense to filing violations and we will rigorously police these sorts of violations through streamlined actions.” It is important for public companies to understand the SEC enforcement staff’s use of quantitative data sources and ranking algorithms to identify individuals and companies with notably high rates of filing deficiencies. In particular, Ceresney pointed to using “quantitative analytics,” which allow the staff to make allegations on a broad scale with limited resources. Richard Hill, “33 Insiders, Companies Settle Late Reporting Allegations in SEC Sweep,” Bloomberg BNA Daily Report for Executives, (September 10, 2014). This is consistent with White’s previous statements that the SEC would harness the power of enhanced technologies as a “force multiplier” in the SEC’s effort to let market participants know that it is “looking and pursuing charges in all directions.”

What the Rules Require When Officers, Directors and Major Stockholders Trade

Section 16(a) and the rules promulgated thereunder require each officer, director, and greater-than-10 percent stockholder (collectively, “insiders”) of a public company to file a Form 4 with the SEC within two business days after the date of certain transactions resulting in a change in beneficial ownership of the company’s equity securities. A Form 5 must be filed with the SEC
within 45 days after the end of each fiscal year for certain types of stock transactions that the SEC has designated as eligible for a Form 5 filing, rather than a Form 4 filing. In addition, insiders must also report on a Form 5 all transactions that occurred during the fiscal year that should have been, but were not, reported earlier on a Form 4.

In general, Section 13(d) and the rules promulgated thereunder require that any person or entity (or group of persons or entities acting together) that makes an acquisition of common stock which results in such person or group owning more than 5 percent of the outstanding shares of common stock of the company, must report the ownership of company securities by filing either a Schedule 13D or Schedule 13G with the SEC.

One principal function of Sections 16(a) and 13(d) is to enable information to rapidly enter the public market about insider transactions and significant changes in stock ownership. Violations of Sections 16(a) and 13(d) do not require a showing of intentional conduct, and a failure to timely file a report, even if inadvertent, constitutes a violation.

**SEC Holds Insiders Responsible for Failing to File, Even Where Companies Took Responsibility for Preparing Reports**

The SEC’s orders with respect to individuals and investment firms generally alleged violations of Section 16(a) of the Exchange Act for failing to timely file reports of transactions on Forms 4 and annual statements of beneficial ownership on Form 5, and of Exchange Act Section 13(d) for failing to file timely reports of beneficial ownership of more than 5 percent of a company’s stock. The penalties for these violations ranged from $25,000 to $120,000. The SEC’s enforcement division will litigate the charges against one individual.

The SEC was not persuaded by the defense raised by many insiders that their delinquent filings resulted from failure on the part of the public company issuer that took on responsibility for the preparation or filing of these reports. The SEC consistently stated in its findings that “the failure by an issuer to inform an insider that he or she is subject to Section 16, and the failure of company personnel to make timely filings on an insider’s behalf after being timely informed of such transactions by the insider, does not excuse an insider’s violations of reporting requirements. An insider retains legal responsibility for filing requirements, insuring the obligation to assure that the filing is timely and accurately made.” See SEC v. Arling, Release No. 73058 (September 10, 2014), fn. 5, available at www.sec.gov/litigation/admin/2014/34-73058.pdf.

In some cases, the SEC specifically noted that respondents took inadequate and ineffective steps to monitor whether timely and accurate filings were made on their behalf.

**SEC Also Takes Public Companies to Task for Failing to Timely Report**

Despite confirming that the responsibility for timely filings ultimately remains with the insider, the SEC also levied fines against six publicly traded companies for (1) being the cause of filing failures by insiders and/or (2) failing to report their insiders’ filing deficiencies. In particular, the SEC alleged that these companies voluntarily accepted certain responsibilities for insiders’ Section 16 filings and then acted negligently in the performance of those tasks, holding such companies liable as a cause of Section 16(a) violations. The SEC noted in almost all of these cases that the issuer had voluntarily agreed with officers and directors to prepare and file reports, but repeatedly failed to perform the agreed-upon tasks on a timely basis and employed procedures that were insufficient and negligent.

The SEC also charged these companies with a failure to comply with Form 10-K and/or proxy statement disclosure requirements regarding late or missing Section 16 filings, which are set forth in Item 405 of Regulation S-K. As a means of increasing compliance by insiders with their reporting obligations under Section 16(a), the SEC’s rules require all public companies to disclose in their proxy statements and annual reports on Form 10-K the names of all insiders who failed to file timely reports during the previous fiscal year, and the number of late or unfilled reports by each such insider. False or misleading Item 405 disclosure can constitute a violation of Section 13(a) of the Exchange Act and Rule 13a-1, which require issuers to include specified information in their annual reports in conformity with SEC requirements. As with Section 16(a) and 13(d), violations of Section 13(a) do not require a showing of intentional conduct. The penalties for these violations ranged from $75,000 to $150,000.

**Lessons Learned**

Issuers and insiders are advised to heed the warnings of White and Ceresney and be proactive in establishing and following procedures for compliance with Sections 16(a), 13(a), and 13(d) and the Form 10-K and proxy statement disclosure requirements in Item 405:

- Insiders bear ultimate responsibility for the timeliness of their filings and must ensure timely and accurate processing and reporting of transactions, even when relying on the assistance of issuers or brokers with respect to such reporting.
- Issuers that assume responsibility for preparing, processing, and/or filing reports for insiders must ensure that they have sufficient policies and procedures in place to timely and accurately complete such filings.
- Issuers must ensure that they have in place policies and practices to facilitate accurate, timely and complete disclosure of late Section 16(a) reports in their annual reports and proxy statements.
- While insiders and issuers always have been advised to make their required filings on time, the SEC now appears more focused on these types of reporting violations than in the past, regardless of whether or not they are linked with other alleged violations.
- More broadly, these actions reflect the SEC’s ability to leverage technology to target an area of concern, and market participants and practitioners should expect to see other examples. Prior to these actions, the SEC had touted such acronyms...
as MIDAS (Market Information Data Analytics System), ABAP (Advanced Bluesheet Analysis Program), CAT (Consolidated Audit Trail), API (Aberrational Performance Inquiry), AQM (Accounting Quality Model), and NEAT (National Exam Analytics Tool) as tools to help the SEC and its staff comb through a variety of information to detect a range of potential illegal activities from insider trading to accounting and disclosure fraud. These efforts reflect the SEC’s strong commitment to significant investment in sophisticated technology to enforce the federal securities laws.

The authors all practice at Wilmer Cutler Pickering Hale and Dorr LLP.
In a recent decision, the Delaware Court of Chancery dismissed a claim that the board of directors of an insolvent Delaware corporation breached its fiduciary duties by pursuing a risky business strategy to benefit the corporation’s sole stockholder at the expense of the corporation’s senior creditors. Quadrant Structured Products Co. Ltd. v. Vertin, C.A. No. 6990-VCL (Del. Ch. Oct. 1, 2014). Although the sole stockholder designated all but one member of the corporation’s board of directors and the corporation’s CEO held the remaining board seat, the court found that the stockholder’s board designees were not conflicted in the decision to change the company’s investment strategy from a risk-off to a risk-on strategy, a change which required the company to amend its operating guidelines and obtain approval from its rating agencies. According to the court, directors of insolvent corporations possess wide latitude to pursue value-maximizing strategies which may benefit all of the corporation’s residual claimants, including its creditors, even if the strategy might ultimately benefit one class of residual claimants more than others. The court also recognized that the corporation’s senior creditors bore the full risk of the risk-on strategy’s failure.

However, the court declined to dismiss claims that the board breached its fiduciary duties to the corporation by authorizing direct and specific payments to the sole stockholder which allegedly transferred corporate assets to the stockholder at the expense of the corporation’s senior creditors. The court further held that these claims would be reviewed under the entire fairness standard of review. Subsequently, on October 28, 2014, the court rejected the creditor’s motion to reconsider its dismissal of the fiduciary claim relating to the board’s adoption of a risk-on investment strategy.

Quadrant is the first decision of a Delaware state court to address a creditor’s claims that the directors of a financially troubled corporation breached fiduciary obligations owed to creditors since the 2007 Delaware Supreme Court decision in North American Catholic Educ. Programming Found., Inc. v. Gheewalla, 930 A.2d 92 (Del. 2007). Gheewalla rejected much of the Chancery Court precedent which had evolved since the landmark decision in Credit Lyonnais Bank Nederland N.V. v. Pathe Communications Corp., C.A. No. 12150, Allen-C. (Del. Ch. Dec. 30, 1991) unsettled corporate boardrooms with its suggestion that directors of distressed corporations must consider creditors’ interests in their decision-making process.

From Credit Lyonnais to Gheewalla
Since the Delaware Court of Chancery’s decision in Credit Lyonnais and earlier decisions applying the trust fund doctrine, Delaware law has recognized that the fiduciary obligations of directors change when the corporation faces insolvency. According to Credit Lyonnais, the fiduciary duties of directors of troubled corporations run primarily to the corporate enterprise as a whole. The directors of distressed corporations are therefore not required to prefer the interests of stockholders to the exclusion of non-stockholder interests, as the law generally requires of directors of solvent corporations. Rather, the board must maximize the value of the entity for the benefit of all of the corporation’s residual claimants, including its creditors. According to Credit Lyonnais, the change in the nature of the directors’ fiduciary obligations occurred prior to actual insolvency at a point in time called the “vicinity” of insolvency. Other cases referred to the relevant transitional moment as the “zone” of insolvency. However, neither Credit Lyonnais nor subsequent decisions articulated a clear test for determining when a corporation was operating in the “vicinity” or “zone” of insolvency. The courts determined actual insolvency by using one of two tests: (1) a traditional balance sheet insolvency test and (2) an equitable insolvency test, the latter of which looked at the corporation’s ability to pay debts as they became due in the ordinary course. Based on Credit Lyonnais, the Delaware courts allowed creditors to pursue direct claims for breach of fiduciary duty against directors of insolvent and nearly insolvent corporations.

In the 2004 decision in Production Resources Group, LLC v. NCT Group, Inc., 863 A.2d 772 (Del. Ch. 2004), the Court of...
Chancery adopted a much narrower view of the Credit Lyonnais decision than any decision to date – finding that Credit Lyonnais did not support the creation of broad rights for creditors to assert direct claims for breach of fiduciary duties against the directors of distressed corporations. In this vein, the court held that creditors of insolvent corporations generally must pursue allegations that the corporation’s board breached its fiduciary duties by depleting corporate assets as derivative, not direct claims. The court left open the possibility that a creditor could bring a direct claim for breach of fiduciary duty if self-interested director action harmed a particular creditor or class of creditors to the benefit of other residual claimants.

Subsequently, in Gheewalla, the Delaware Supreme Court held that creditors may not bring direct claims against directors for breach of fiduciary duty under any circumstances. The court expressly rejected the contrary dictum in Production Resources Group, LLC and held that directors of insolvent corporations do not owe direct fiduciary obligations to creditors. In the court’s view, Delaware’s common law does not need to afford creditors fiduciary protection because creditors may protect their investments with contractual agreements and are afforded protection under fraudulent conveyance, bankruptcy, and general commercial laws. However, the court held that creditors of insolvent (but not nearly insolvent) corporations may pursue derivative actions to enforce the fiduciary duties that the directors owe to the corporation itself as the primary constituency injured by fiduciary breaches that diminish the corporation’s value.

Post-Gheewalla: Quadrant Structured Products Co. Ltd. v. Vertin

In Quadrant, the Delaware Court of Chancery applied Gheewalla to direct and derivative claims brought by a creditor of an insolvent Delaware corporation against the corporation’s directors and its sole equity holder for breach of fiduciary duty. The defendant in this action was Athilon Capital Corp., a credit derivative product company. Prior to the 2008 financial crisis, Athilon guaranteed credit default swaps on senior tranches of collateralized debt obligations written by a wholly owned subsidiary. Under the company’s operating guidelines, Athilon only could invest in highly-rated, short-term debt securities. Athilon’s business initially was funded through $100 million in equity and $600 million in long-term debt, consisting of $350 million in senior subordinated notes, $200 million in subordinated notes, and $50 million in junior subordinated notes. During the financial crisis, Athilon lost an AAA/Aaa credit rating, its securities traded at deep discounts and Athilon largely lost the ability to operate its business. In 2010, defendant EBF & Associates, L.P., acquired all of Athilon’s equity, some of its junior notes and the right to designate four directors, two of whom also were EBF directors, to Athilon’s five member board. In 2010, an EBF affiliate began providing services to Athilon for $23 million a year, a price which far exceeded the market rate of $5–7 million. In May 2011, Athilon received approval from its rating agencies to amend its operating guidelines to permit the company to invest in high-risk, long-term securities. In May and July 2011, Quadrant acquired Athilon senior subordinated notes and subordinated notes.

In October 2011, Quadrant filed the complaint in the present action and sought relief for breach of fiduciary duty as a creditor of Athilon. Quadrant alleged that the Athilon directors: (1) adopted a business strategy of making speculative investments to benefit EBF at the expense of Athilon’s senior creditors who would bear the entire risk of the strategy’s failure; (2) continued to pay interest on EBF’s junior subordinated notes, which were underwater, despite having the ability to defer payments without repercussions; and (3) paid excessive licensing and servicing fees to an EBF subsidiary at above-market rates. According to Quadrant, the directors breached their fiduciary obligations to Athilon’s creditors by authorizing the foregoing actions to EBF’s benefit. Defendants moved to dismiss Quadrant’s complaint for, inter alia, failure to state a claim. In reviewing Quadrant’s claims, the court reiterated that post-Gheewalla, directors of an insolvent corporation do not owe direct fiduciary obligations to the corporation’s creditors. Rather, as the principal constituency injured by fiduciary breaches that diminish the firm’s value, creditors of an insolvent corporation may pursue derivative claims for fiduciary breaches that deplete the value of the corporation’s assets. Thus, the court left open the possibility that Quadrant lacked derivative standing because some of the challenged transactions pre-dated Quadrant’s acquisition of Athilon’s debt – holding that the contemporaneous ownership requirement in Section 327 of the Delaware General Corporation Law did not apply to creditors.

Quadrant argued that its claims must be reviewed by the court under the entire fairness standard and could not be resolved on a motion to dismiss. Specifically, Quadrant argued that a majority of Athilon’s directors were conflicted in the decision to embark on a risk-on strategy. The court disagreed. According to the court, business decisions which affect the value of the entity as a whole, without conferring specific benefits on the directors themselves or, in the case of dual fiduciaries, on the competing beneficiaries of fiduciary duty, are reviewed under the deferential business judgment standard of review. The court explained that when directors make decisions that appear rationally designed to increase the value of the firm as a whole, “Delaware courts do not speculate as to whether those decisions might benefit some residual claimants more than others.” The court concluded that “directors are not deemed conflicted on the theory that a riskier business strategy will benefit EBF and harm Athilon’s creditors.”

In contrast, the court found that plaintiff had stated a claim that Athilon’s board breached its fiduciary duties by failing to...
defer the payment of interest on the junior notes held by EBF and by paying excessive service and licensing fees to an EBF subsidiary. With respect to the interest payments, the complaint alleged that: (1) the Athilon board had the ability to defer payment of interest on the junior notes, (2) EBF owned all of the junior notes, and (3) as the holder of the junior notes, EBF would not have received anything in an orderly liquidation. The court held that this claim would be reviewed under the entire fairness standard of review because the payment effectively transferred value owed by all residual claimants of Athilon’s assets to the party in control of Athilon, EBF. With respect to the alleged payment of excessive licensing and service fees to an EBF affiliate, the court stated: “EBF stands on both sides of the transaction, making entire fairness the governing standard of review with the burden of proof on defendants.” Accordingly, the court declined to dismiss plaintiff’s claims relating to the alleged payment of excessive licensing and service fees to an affiliate of EBF and the failure to defer interest payments on the junior notes.

Conclusion

Quadrant reaffirms that directors of insolvent corporations have considerable latitude to pursue value-maximizing strategies which are designed to benefit the corporate enterprise as a whole absent evidence that some compelling personal interest tainted the decision-making process. According to the court, its decision was analogous to prior precedent upholding, under the business judgment standard of review, decisions of directors of solvent, but controlled corporations which affected all stockholders equally, such as the declaration of a pro rata dividend. However, it should be noted that board decisions which have facially treated the minority and a controller equally, but which have served some extraneous interest of the controller, such as a desire for liquidity, have been reviewed under the entire fairness standard of review. It seems questionable whether the risk-on strategy equally affected EBF and Quadrant and whether the decision fits under the “equal treatment” rubric. The decision seems more a product of the decisions in the Revlon context which have protected directors in their good faith, but imperfect attempt to carry out their Revlon duties of value maximization.

The court’s application of the business judgment rule to the issue of value maximization despite the presence of a controller, a controlled board, and a finding that plaintiff’s other fiduciary claims survived a motion to dismiss underscores the deference accorded by Delaware law to directors of insolvent corporations. In late October, Quadrant moved to reargue the dismissal of its fiduciary claim regarding the board’s adoption of a risk-on investment strategy. The Court of Chancery swiftly denied the motion, reaffirming its prior decision.

Lisa R. Stark is a partner in K&L Gates LLP’s Wilmington, Delaware, office. The statements and views expressed herein are solely those of the author and do not reflect those of K&L Gates LLP or any of its other attorneys, are intended for general informational purposes only, and do not constitute legal advice or a legal opinion.
Ethics Corner: Be Very Quiet . . . I’m Hunting Jurors: Social Media and Ex Parte Communications

By Stuart Teicher

Whether we are in-house attorneys or outside counsel, all business lawyers try our hardest to avoid disputes. Sometimes things fall apart, however, and we find ourselves navigating the waters of litigation. Very often, proper preparation for litigation demands that we investigate a myriad of parties. These days, one of the tools at our disposal is social media. There is a treasure trove of information available about adverse parties and witnesses. While the standards for acceptable conduct are relatively straightforward (hint: stay away from “deception”), a monkey wrench is thrown into the proverbial machine when we consider the implications of investigating a particular litigation target – potential jurors. A relatively recent opinion from the New York City Bar Association on the topic caused a bit of an uproar in the ethics world.

Ex parte communications with prospective jurors and members of a sitting jury have long been prohibited. New York City Bar Association, Formal Opinion 2012-2. Also see NY Rule 3.5(a) and (b). But the advent of social media has created a difficult wrinkle because lawyers are using social media to research both prospective and sitting jurors. That isn’t frowned upon, per se. In fact, the New York City Bar Association recognized that this type of research is consistent with a lawyer’s fundamental duties. It noted that, “… standards of competence and diligence may require doing everything reasonably possible to learn about the jurors who will sit in judgment on a case.”

The problem is that part of the lawyer’s investigation process through social media could include communicating with the jurors, thereby violating Rule 3.5(b). There could be friending, exchanges of messages, or a lawyer might just observe a juror’s social media page. The issue is trying to figure out which of those actions actually constitute a “communication” that violates the rule. The authorities are concerned because “social media . . . can blur the line between independent, private research and interactive, interpersonal ‘communication.’”

The City Bar didn’t make many waves when it opined that “friending” a juror constituted a prohibited communication. That’s pretty much a no-brainer. It shook things up slightly, however, when it stated that simply researching a juror’s social media page could constitute a communication.

The Bar was concerned about situations where a lawyer researches the juror’s page and the website sends a message to the juror letting them know that the lawyer viewed the page. How could this happen? Consider this: LinkedIn automatically generates a message that tells a user who has viewed the profile recently. The City Bar considered those type of platform-generated messages to be “communications.” In the Bar’s view, the key factor was the effect that such knowledge would have on the recipient (in this case, the juror). The Bar held, “it is the ‘transmission of,’ ‘exchange of’ or ‘process of bringing’ information or ideas from one person to another that defines a communication,” and that in the world of social media, “this focus on the transmission of information or knowledge is critical.” In a situation where a juror was notified that a lawyer was viewing the juror’s social media page “…the researcher imparted to the person being researched the knowledge that he or she is being investigated.” The City Bar believed that “the transmission of the information that the attorney viewed the juror’s page is a communication that may be attributable to the lawyer and even such minimal contact raises the specter of the improper influence and/or intimidation that the Rules are intended to prevent.” In addition to being intimidating, the knowledge of that research might “tend to influence the juror’s conduct with respect to the trial.” (This quote actually comes from a different opinion out of New York City – NYCLE Committee on Professional Ethics, Formal Opinion No. 743, issued May 18, 2011, at 3) Thus, the key question is whether the juror would have learned of the lawyer’s research. NYC Opinion 2012-2 at 3.

Note that the City Bar made a distinction between whether the lawyer knew that the notice would be generated, or whether it was unknowingly or inadvertently sent. The former was considered to be a clear violation of the rules, but the Bar wouldn’t say if they thought that the rules were broken.
if the message was sent by the social media page inadvertently. They said it “might constitute a prohibited communication even if inadvertent or unintended.” Either way, they see the communication as a no-no.

But – lest you think that the ethics world is a boring place – there is a bit of controversy on the topic. The ABA has also opined on the topic and came down with a contradictory result.

In Formal Opinion 466 (April 24, 2014), the ABA’s Standing Committee on Ethics and Professional Responsibility evaluated the same question that the City Bar considered. Knowing that Rule 3.5 prohibits communications with jurors, they considered whether a lawyer could investigate a juror’s social media page. The ABA Committee resolved the easy question the same way as the City Bar (overt contact like friending is a prohibited communication). The ABA Committee came down differently, however, on the tough question – whether a lawyer may passively review a juror’s social media page if that review will become known to the juror. In that scenario, the ABA Committee disagreed with the City Bar. The ABA Committee thinks it’s okay.

According to the ABA Committee, a lawyer is not communicating with a juror when a website sends an automatically generated notice to the juror telling them that the lawyer was reviewing their website. They stated, “This Committee concludes that a lawyer who uses a shared ESM platform to passively view juror ESM under these circumstances does not communicate with the juror. The lawyer is not communicating with the juror; the ESM service is communicating with the juror based on a technical feature of the ESM” (“ESM” stands for “electronic social media” in this opinion). What’s amazing is . . . that’s it. The opinion is almost devoid of analysis. The only statement that in any way resembles some deeper thought is an analogy. The opinion states, “This is akin to a neighbor’s recognizing a lawyer’s car driving down the juror’s street and telling the juror that the lawyer had been seen driving down the street.”

When a lawyer passively investigates a juror’s social media page, that lawyer is reading the details of the page. They are inspecting the contents and looking for information. It’s a lot less like driving down the street near a juror’s house and lot more like standing on the juror’s lawn peering over their bushes through the picture window in their living room, or rifling through the juror’s garbage cans. I believe it’s more intrusive than the drafters of the opinions make it out to be. And intrusive can be intimidating.

But the ABA Committee never talked about the potential intimidation. They failed to explore that key underlying issue at all. They simply made a distinction about who is actually initiating the communication. Since the website sent the message, it’s not a lawyer communication. The mistake the drafters are making is focusing on the technical manner in which the message is sent. The issue is not about who (or what) sent the communication, rather, it’s about what triggered that communication. The impetus for the system sending a communication to the juror was the lawyer’s research. The website-generated communication was only triggered because the lawyer made an appearance on the juror’s webpage. The lawyer’s snooping caused the message to be sent.

The concern that prompted the City Bar opinion was the fact that knowledge of the lawyer’s presence on the juror’s social media page could be intimidating. The message, regardless of who sent it, makes the juror aware that they are being watched. The key factor to the City Bar was the effect that such knowledge would have on the recipient (in this case, the juror). That’s why they stated that “even such minimal contact raises the specter of the improper influence and/or intimidation that the Rules are intended to prevent.”

To date, there haven’t been any other states that have chimed in on the matter.

I would expect that when other states opine on the matter that they will review the rationale behind the City Bar opinion in a more meaningful way, and it will be interesting to see how they decide.

Stuart Teicher is a professional legal educator and the author of the book, Navigating the Legal Ethics of Social Media and Technology, published by Thomson Reuters (June 2014). “Ethics Corner” is sponsored by the Professional Responsibility Committee, and is edited by Robert Evans III, a partner at Shearman & Sterling LLP.
In so many ways, Alex Dimitrief’s story epitomizes the American dream. Not knowing any English, his parents left Russia and immigrated to Montreal, then moved to Illinois. The Russian immigrants watched their son attend top schools, first, Yale, where he graduated summa cum laude, then Harvard Law School, where he graduated magna cum laude. He even landed at the White House as a White House Fellow in the Reagan Administration’s Office of Political and Intergovernmental Affairs, the youngest ever Fellow at that time.

Now Alex Dimitrief is Senior Vice President and General Counsel at GE Capital. Prior to going in-house, he was a trial lawyer at Kirkland & Ellis. His practice spanned many industries, including securities, intellectual property disputes, environmental matters, product liability, and bankruptcy litigation.

* * *

You were at Yale as an undergraduate and earned a degree in economics and political science. Were you once considering business or politics? I was seriously considering politics. I had a real admiration for a lot of leaders that I grew up working with. My first real boss was Ed Madigan, our congressman from Lincoln, Illinois. I always had a strong interest in public service and I thought that that was something that I’d want to do at some point. I still remain interested in public service, but I lost my appetite in politics when I saw how much of it was all about begging for money.

I remember helping Chuck Percy, who was the senator from Illinois at that time; I got involved in one of his reelection campaigns. I’ll never forget when Ed Madigan said how sad it was to watch a guy like Chuck Percy, who was this national figure and a renowned person, have to spend five or six hours a day on the phone, calling people and dialing for dollars.

You ultimately decided to become a lawyer. How did you make this decision? I always like public speaking. I did debate in high school, and, as my parents would say, arguing points came a little bit too naturally to me.

But my real passion when I was in high school and college was math and computer science. In fact, at college, I worked with a guy at the University of Illinois and we wrote an interactive game that could be played in schools by kids called “Word War.” I actually got some royalties from it.

But my dad was convinced there wasn’t any money to be made in computers. And so he really strongly steered me towards law. There’s always a moment when I wonder about that decision not to go into high technology.

But having become a lawyer, I love it. I think it’s a great opportunity to really do a lot of great things.

You graduated magna cum laude from Harvard Law School. When you look back at that time, what does Harvard do well in terms of preparing you for practice? It’s a cliché, but law school really teaches you how to think. I believe that lawyers are trained very well in terms of being presented with complicated problems and measuring those problems against a set of principles that guide a rational decision that’s consistent with the rule of law and will lead to a good outcome.

That’s why legal training in law schools is good for any variety of professions, not just lawyers. Some of the best CEOs, some of the most successful private equity managers that I’ve known, have all had legal training. Law school equipped them with an approach towards distilling a complicated situation to several basic principles and coming out with the right answers.

Who was among the professors at Harvard influenced you most? Professor Clarke Byse. I believe he was the real world professor who served as the model for Professor Kingsfield in the Paper Chase. He was known as a very strict professor, and he was known as having a very autocratic method in his class. But beneath it all, Professor Byse cared deeply about his
students. And what he really cared about was making sure you left his classes having learned how to think like a lawyer. When I was there, he taught Administrative Law. With all due respect to people who specialize in Administrative Law, there probably aren’t many topics that are more boring, but Professor Byse was able to bring it to life because it was really more about how to reach decisions in the right way. He took the approach: how should federal agencies afford people due process when they’re reaching decisions about things that affect their lives?

Although the cases were dry, although the statutes we were dry, the discussions we had really were animated. It showed what a great professor could do in terms of engaging with students and getting your students to really think.

You were a White House Fellow in the Reagan Administration’s Office of Political and Intergovernmental Affairs. What did you do? Are there highlights? The White House Fellows program was a remarkable opportunity. I was 27, and I believe I was the youngest ever White House Fellow of that time. It had two aspects to it: the first was the actual job part of it, which I’d say was 90 to 95 percent of what I did. I was fortunate enough to be assigned to Mitch Daniels, who at the time was the special assistant to president Reagan for political and intergovernmental affairs.

Mitch served as President Reagan’s liaison to governors, mayors, and state representatives. He also served as President Reagan’s liaison to the Republican Party.

It was really about working with local governments to make sure their considerations and needs were being taken into account by the federal government, in terms of shaping policies. For a Republican administration that believed in federalism, it was a pretty exciting time to be there.

I was also helping the Republican candidates for governor or the Senate get in synch with President Reagan’s policies and helping to communicate President Reagan’s policies to the Republican party.

Mitch was an incredibly capable person. This was a relatively early stage in his career and I got to see him do remarkable things there. He was able to bring people along by being persuasive and setting a strong example. It’s no accident that he went on from there to be a senior executive at Eli Lilly and the Hudson Institute. And then of course, he came back to Washington to be President Bush’s OMB director and then went on to be a very successful governor of Indiana.

A real highlight was to see President Reagan. I was fortunate enough to be able to interact with the president on a number of occasions. The best highlight had to be when I was able to introduce President Reagan to my dad. President Reagan knew I was a first generation American. He said to my dad how great it was that somebody could come to this country not knowing English, and then 27 years later, have their son graduate from great schools and be able to work for the president of the United States. My dad was just smiling from ear to ear.

What country are you from originally? I was born in Montreal, and then we moved to Illinois when I was about a year-and-a-half old. But my parents were both Russian. My mom immigrated right after World War II, and my dad came over to Canada in the early 1950s, and they met in Montreal.

You were also an Honors Intern at the Department of Justice. I was only there for three months, but I worked in the solicitor general’s office. I hadn’t even passed the bar exam yet, but I just dived in and got involved in three or four cases involving federalism and abortion rights.

It was my first exposure to the intersection between political appointees and the career professionals who work at the Justice Department, and that was fascinating to witness.

Eventually you ended up in private practice at Kirkland & Ellis from 1986 until 2007 as a trial lawyer. What did you enjoy about that private practice area and is there a case that stands out from that time? What I enjoyed the most were two things. I had great teams. As I became a more senior lawyer, I really enjoyed working with young lawyers and watching them put on their first witness and cross-examine their first witness.

I also enjoyed the writing. I’m one of these lawyers who believes that writing is increasingly becoming a lost art. If there’s one comment I have for young lawyers who are entering the profession today, writing is 90 percent of what we do. It’s your chance to influence judges before the first argument. It’s your chance to make a first impression with your case.

What makes a great trial attorney? Integrity and authenticity. It’s owning up to the weaknesses in your case and being able to transparently put the strengths and weaknesses out there in a way that persuades people to come along with you. You have to be quick on your feet; you have to be articulate; but I think the most important things are integrity and authenticity.

The way that I always explain it to people is that, in the course of the trial, when a judge needs to know what’s really the answer to something, you want the judge to look to you. And if you can pass that test, you’ve done a good job as a trial attorney.

In 2007, you left private practice and joined GE as a vice president for litigation and legal policy. What made you decide to go in-house? It was something that I had never really planned to do. I was very happy at Kirkland & Ellis. Then out of the blue, I got this opportunity. I really had to think hard about it. I made the switch for two reasons: I had been able to accomplish a lot of things while I was at Kirkland & Ellis and so I was ready for a change. I also looked at GE as an opportunity to switch from one great institution to another. I’ve never looked backed since.

What’s the biggest difference between in-house and private practice? I suppose that when I was a younger lawyer, I would have said an in-house practice seemed easier. Less stress, better hours. I’m sorry to say that’s no longer the case. I
think the biggest difference, and it’s going to sound negative but it really isn’t, is that you go from a law firm where it’s all about the lawyers and what you do, to a company where you are an enabling function in the most noble sense of the word. We help the company do things in legal ways that honor our ethical obligations to all of our stakeholders.

What advice would you give to a lawyer in private practice who is thinking of going in-house?
I’d tell the lawyer that she or he ought to be sure that you’re going to a company you can believe in, you can be proud of and passionate about.

In 2011, you were appointed as vice president and general counsel of GE Energy. How is that position different from your previous one?
When I first went in-house, it was the flip-side of what I was doing at Kirkland & Ellis. I was in charge of litigation for GE and all its business units, the compliance team, and internal investigations.

When I became general counsel of Energy, I became responsible for all legal aspects of the overall business strategy. And the great thing about the Energy job was that, at that time, we had a lot of acquisitions, joint ventures, and other business deals.

The luxury of being the general counsel of the business is you get to play offense as well as defense. Now I’m at GE Capital and here too I help formulate overall strategy as well as litigation strategy.

You wrote a chapter about billing for the book, Successful Partnering Between Inside and Outside Counsel. Can you briefly summarize your main points?
The point I tried to make was that too many law firms make the mistake of relegating their budgeting and billing to clerical assistants, and the lawyers themselves never look at budgets or at bills. They view them as a nuisance. And boy, they’re making a big mistake when they do that.

I’m willing to bet you that 95 percent of the people who are reading this interview don’t review bills very carefully before they go out to their clients, and that’s just an enormous mistake because the care and attention that you pay to these issues return dividends.

I also have a little private campaign going on to displace the hourly rate, but it’s not because I think the hourly rate is inherently evil. I think there’s something a little bit off about a business that bills itself and gets paid on time alone as opposed to talent.

How have you benefited from your membership in the ABA, especially the Business Law Section?
The meetings that I have been able to attend provide a chance to hear some of the best lawyers who are out there talk about the big issues that are confronting us.

I will say it frustrates me to no end when I’m on a panel and I look out and I see everybody reading their Blackberrys and iPhones. I’m guilty of that too sometimes. But we as a profession ought to take a collective pledge to leave our iPhones or Blackberrys back at the office when we go to meetings like that so we can really benefit from interacting with each other.

You served as a member of the board of directors of the Constitutional Rights Foundation Chicago, which educates poor children that invites and encourages them to become active citizens. How did you get involved and what did you enjoy about this experience?
I’ve always had a passion for education and the power of ideas. A great strength of the United States is that we resolve issues, for the most part, through the strength of ideas. The Foundation is about educating children about the power of ideas and the privileges that they have as citizens of the United States where democracy decides things. It’s just a tremendous organization. It also empowers public school teachers by providing curriculums and training to help teachers educate kids.

You’re also a big supporter of the Ronald McDonald House. How did you become involved?
That goes back to my days at Kirkland & Ellis. McDonald’s was an important client of mine and I quickly came to believe in the mission of the Ronald McDonald House Charities. They do an enormous service to families, by making housing and comfortable facilities available for families to stay near their children who are getting treatment in hospitals.

When my wife and I moved out to Connecticut to take the new job at GE, I was in search of a charity. I sought out the Ronald McDonald House in New York, and I’m glad that they welcomed me and they put me on their board. I love the mission of the House.

I also hear you’re a huge St. Louis Cardinal and Chicago Blackhawks fan.
I hear you have season tickets to the Cardinals.
When I tell people that I have season tickets to the St. Louis Cardinals, even though I’ve never lived in St. Louis a day in my life, people look at me like I have a hole in my head. I can blame this one on my wife, because I happened to pay a fortune for a ticket to the World Series game in 2004. My wife said that if I was going to buy that much to go to one game, then I ought to just buy season tickets. I actually took her up on it. I think Jill regrets having suggested it.

Thank you so much for your time.
Recent Committee Meetings
Several Committees of the Business Law Section have recently held stand-alone Committee meetings.

Business Bankruptcy:
The Business Bankruptcy Committee met on October 8, 2014, in conjunction with the National Conference of Bankruptcy Judges. An incredible lineup of programming included:

- (Almost) Everything You Wanted to Know About . . . Executory Contracts
- Recent Developments Regarding the Interface Between Insurance and Bankruptcy
- Discovery and Judicial/Legislative Developments in Mass Torts and Asbestos Trusts
- Engagement Agreements with Individual Chapter 11 Debtors
- Herding Clients: Working with Multiple Secured Creditors
- Is there Room in the Chapter 11 Ark for Trustees, Examiners, Receivers, and CROs?
- It’s Not about the Money! (or Is It?): Garnering Support for Bankruptcy Sales Without Increasing the Purchase Price
- Pro Bono Service on a Board of a Not-for-Profit in Crisis/Fulfilling Your Not-for-Profit’s Mission During Financial Distress
- Restaurant Bankruptcies – Should I Make a Reservation Now?
- Take the First Exit! – Defenses That Can Win a Case Early
- The Uniform Voidable Transactions Act
- What Every Distressed Investor Should Ask When Venturing Offshore – Are Chapter 11 Skill Sets and Experience Alive and Well (and Relevant) in Europe?

The program materials and audio for each of the presentations can be found here.

LLC’s, Partnerships, and Unincorporated Entities:
The Third Annual LLC Institute, was presented by the Committee on LLC’s, Partnerships, and Unincorporated Entities in Arlington, Virginia, on October 16–17, and was a great success! Programming included:

- Family Business Disputes
- Indemnification and Advancement
- Jewel v. Boxer and Law Firm Failures
- LLC Case Law Update
- LLC Series Drafting Project
- Limited Liability – How Far Does It Go?
- Real Estate Ventures, TICs
- USA Cafes

All of the program materials, as well as PowerPoint presentations and audio recordings, are available here.

Recent Committee Newsletters
Many Committees have also recently published newsletters, including the Business Tax Quarterly, published by the Taxation Committee, which includes the following articles:

- New Rules on Tax Allocation between Banks and Bank Holding Companies: Who Owns Tax Refunds?
- Tax Court Provides Guidance on International Governments Acting Collectively and § 162(f)
- Inversions
- Michigan Supreme Court Approves MBT Refunds Based on MTC Election
- The MTC Election Made by IBM
- Another Look at U.S. Federal Income Tax Treatment of Contingent Earnout Payments
- Uncashed Settlement Checks Paid to Charity Under Court-Approved Settlement Cannot Be Escheated, Texas Supreme Court Rules

The Consumer Financial Services Committee published its Fall Newsletter with features including:

- Member Spotlight on Robert N. Collier and the Leadership Diversity Outreach Committee
- A New Model for Pro Bono: The “Pillar Firm”
- California Law Exempts Nonprofit Lenders to Help Build Consumer Credit
- Debt-Sale Compliance: New Guidance from OCC Requires Action
The Community Economic Development Committee Newsletter was published on November 4, 2014, and can be found here. The newsletter highlighted its webinar on Form 1023EZ which was held on Tuesday, November 18th, and introduced the Committee’s directors.

The Nonprofit Organizations Committee also published its newsletter on November 4, 2014, which can be found here. The newsletter includes the following articles, reports, and updates:

- Enterprise Risk Management for Nonprofit Organizations: Meeting Challenges to Tax-Exempt Status
- Religious Organizations Subcommittee Report
- Nonprofit Governance Subcommittee – Disaster Planning Discussion
- Task Force Governance of Social Benefit Entities – Annual Meeting September 11, 2014
- Nonprofit Attorney Profile: Mohamed Sabur, Director, Program to Strengthen Muslim Charities at Muslim Advocates
- National Updates
- State Updates

The Cyberspace Law Committee published its November 2014 Newsletter on November 13, 2014. The newsletter includes registration information and highlights of the Cyberspace Law Institute and Winter Working Meeting to be held on January 23–24, 2015, in Charlotte, N.C., at the Omni Hotel, as well as a preview of scheduled CLE programming to be presented by the Committee at the Business Law Section’s Spring Meeting in San Francisco on April 16–18, 2015.

Upcoming Events

Fall Meeting:
The Business Law Section Fall Meeting will be held November 21–22, 2014, in Washington, D.C., at the Ritz-Carlton Washington D.C. The Fall Meeting provides comprehensive business law programming, including:

- More than a dozen CLE programs prepared and presented by practice-area experts
- Up-to-the-minute topical sessions covering the latest business law issues relevant to your practice
- Social events designed to facilitate networking with new contacts and reconnecting with old friends

Committees holding meetings and presenting CLE programs include Business and Corporate Litigation, Career and Practice Development, Corporate Governance, Corporate Social Responsibility Law Task Force, Employee Benefits and Executive Compensation, Federal Regulation of Securities, Government Affairs Practice, Institutional Investors, Law and Accounting, Legal Opinions, Middle Market and Small Business, Professional Responsibility, and Securitization and Structured Finance.

We hope to see you there. If you cannot attend in person, please dial in to the Committee meetings. The schedule for the Fall Meeting, including dial-in information, can be accessed here.

In The Know:
On December 11, 2014, 1:00 – 2:30 p.m. Eastern (12:00 – 1:30 p.m. Central), the Mergers and Acquisitions Committee will present “Cases Do Matter: Judicial Forces Shaping M&A Deal Terms.” This program will explore:

- Recent judicial decisions affecting M&A deal terms, such as those interpreting merger agreements or state law applicable to transactions
- The impact on language and negotiating positions in merger agreements resulting from the judicial decisions
- Market trends from the Deal Points Studies that illustrate how practice is changing because of the judicial decisions
- How law firms can effectively share this kind of information among their lawyers to better serve clients

In The Know is an exclusive Business Law Section member benefit, and you can earn free business law CLE by attending these hot-topic webinars developed by industry experts. Click here to register for the M&A Committee’s presentation.
Business Law Today Board Members 2014–2015

Co-Chairs:

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

Christopher J. Rockers
Husch Blackwell LLP
christopher.rockers@huschblackwell.com

Advisor:

Robert Boehm
Steiner Leisure Limited
bobb@steinerleisure.com

Members:

Katherine Simpson Allen
Stites & Harbison, PLLC
katherine.allen@stites.com

Phillip J. Long
Branch Banking and Trust Company
pjlong@bbandt.com

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

Kathleen S. McLeroy
Carlton Fields
kmcleroy@carltonfields.com

Michael St. Patrick Baxter
Covington & Burling LLP
mbaxter@cov.com

Bradford K. Newman
Paul Hastings LLP
bradfordnewman@paulhastings.com

Lawrence A. Goldman
Gibbons P.C.
lgoldman@gibbonslaw.com

Michael K. Reilly
Potter Anderson & Corroon LLP
mreilly@potteranderson.com

Kristin A. Gore
Carlton Fields Jorden Burt
kgore@cfjblaw.com

Jeffrey W. Rubin
Financial Accounting Foundation
jwrubin@f-a-f.org

Nicole Harris
Pacific Gas and Electric Company
ndh1@pge.com

John H. Stout
Fredrikson & Byron, P.A.
jstout@fredlaw.com

Kathleen J. Hopkins
Real Property Law Group, PLLC
khopkins@rp-lawgroup.com

Thomas W. White
Wilmer Cutler Pickering Hale and Dorr
thomas.white@wilmerhale.com

Lisa R. Lifshitz
Torkin Manes LLP
llifshitz@torkinmanes.com

Editor:

John Palmer
ABA Publishing Periodicals
john.palmer@americanbar.org