
BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Our Mini-Theme: Cyberspace Law

The [Cyberspace Law Committee](#) gathers annually at its [Law Institute & Winter Working Meeting](#) on the Law of Cyberspace to showcase the latest cyberlaw developments, this year on January 20 at the Hotel Kabuki in San Francisco (registration available [here](#)). For almost 20 years, the committee has been working to analyze legal issues affected by the implementation of emerging technologies and to facilitate the creation of legal infrastructures that protect and support commerce in the digital world. To highlight the committee's cutting edge work, this mini-theme looks at recent proposed legislation, regulation, regulatory guidance, and caselaw, both within the United States and globally, that could dramatically affect the way business is conducted online and in connection with online communications.

First, Professor Jon Garon offers a discussion of two of the most wide-reaching efforts to regulate the Internet to have been introduced in Congress in recent years, in his report on the latest legislative

salvos in the content creators—content distributors wars, the recent Pro-IP Act and the Stop Online Piracy Act. Next, Hank Judy and David Satola consider some of the pressures on a fully free and open global network from some of the non-U.S. sources pushing for more international Internet regulation and control in their piece, “*Business Interests Under Attack in Cyberspace: Is International Regulation the Right Response?*” Next, Sarah Jane Hughes and Roland Trope provide a picture of some of the potentially damaging unintended consequences of the SEC's recently-issued guidance concerning corporate data security practices, in their timely essay “*Avoiding Unintended Consequences Under the SEC Staff's 'Cybersecurity Disclosure' Guidance.*” Finally, Kathy Porter considers how employers can incorporate employee use of mobile communications devices into their employee electronic communications or Internet-usage policies, along with an updated analysis of how some courts have

treated employer efforts to access data stored or created on employee devices, in “*Going Mobile: Are Your Company's Electronic Communications Policies Ready to Travel?*” Each of these pieces illustrates how lawyers, regulators, courts, and employers react to cyberspace developments in ways that can have far-reaching, likely unintended, consequences.

Join the Cyberspace Law Committee's [Winter Working Meeting](#) on January 20, 2012, at the Hotel Kabuki in San Francisco, for five hours of CLE on a variety of current cyber law topics, and plan to stay for open roundtable discussions, breakouts to participate in ongoing committee research and writing projects, and keynotes from special guests from the technology law trenches later on January 20 and 21. The committee's Winter Working Meeting is not to be missed!

[Jonathan T. Rubens](#)
Chair, Cyberspace Law Committee

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

New Legislation Renews Conflict Between Content Creators and Content Distributors

By [Jon M. Garon](#)

In November, Congress began hearings for H.R. 3261, the Stop Online Privacy Act (SOPA). The proposed legislation is the House alternative to the recently passed Senate Bill S.968, PROTECT-IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011). Each of these proposals seeks to continue improving enforcement mechanisms against online intellectual property infringement, particularly involving activities that allude traditional jurisdiction.

The proposed legislation has proven quite controversial, with tech industry leaders Google and Microsoft lining up against the legislation while media companies, AFL-CIO and the U.S. Chamber of Commerce strongly support the bills.

This is not the first time Congress has sought to expand jurisdiction over illegal online activities in recent years. In 2008, Congress enacted the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (the PRO-IP Act). Under this law, civil awards were increased, civil actions were added to the powers for the Department of Justice, and the position of Intellectual Property Enforcement Coordinator (IPEC) was created to serve within the executive office of the president. Victoria A. Espinel was appointed as the initial IPEC.

The PRO-IP Act doubled damage provisions for trademark counterfeiting, making the range \$1,000 to \$200,000

and up to \$2,000,000 in cases of willful counterfeiting. The law also clarified and codified the trademark law interpretation that indirect trademark infringers are subject to the same liability as direct infringers. Copyright law enforcement was also increased, including the ability to seize the books and records of the infringer in addition to the infringing articles. This additional remedy provides law enforcement and civil litigants a powerful tool to track the source of distribution for illegally distributed works.

Perhaps the most potent provision of the PRO-IP Act, however, was the addition of a new seizure provision added to Title 18 of the United States Code, replacing section 509 of the Copyright Act. Section 2323 provides “[a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense . . .” is subject to seizure and forfeiture. The authority is quite broad because the facilitation language could extend to every music player and any website actively promoting infringement.

Last year, the authority under §2323 (and section 18 U.S.C. §981—a broader forfeiture and seizure statute) were used by Immigration and Customs Enforcement (ICE) to seize 90 domain names and counterfeit goods through two separate raids. According to the 2010 annual report of IPEC, the value of goods seized in Fiscal 2010 was significant: “The domestic value of the seized goods—i.e., the value of the

infringing goods, not the manufacturer’s suggested retail price (MSRP) for legitimate product—was \$188.1 million. The estimated MSRP of the seized goods—i.e., the value the infringing goods would have had if they had been genuine—was \$1.4 billion.”

Despite these successes, the impact of the PRO-IP Act is somewhat limited. This is a fraction of the goods counterfeited and media content illegally distributed. As described by Stephen J. Zralek and Dylan Ruga in their January/February 2009 issue of *Landslide*, “it is doubtful” that increased damage awards “will have much effect on the counterfeiting industry because counterfeiters, in general, are difficult to catch and rarely are capable of satisfying a judgment. Indeed, most counterfeiters operate out of back alleys or anonymous storefronts on the Internet; they are transient and disappear easily when caught.”

Frustrated by the limited effect of existing laws, Congress and the White House continue to seek to do more. President Obama has called for greater action, stating in a March 2011 speech “we’re going to aggressively protect our intellectual property. Our single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century.”

But as IPEC director Espinel noted in her 2010 annual report, “[t]here is exten-

sive debate about the government's role in Internet policy in general and the enforcement of intellectual property rights in the online context in particular." Perhaps nowhere is that debate more heavily concentrated than the extension of the PRO-IP Act through additional legislation.

Professor James Grimmelmann of New York Law School summed up the tension over SOPA quite elegantly: "To supporters of SOPA . . . the best way to support 'innovation' and 'creativity' is stronger enforcement, in particular against Internet and financial intermediaries. But SOPA's opponents would say that Obama has the logic exactly backwards: Among the bill's dangers is that it could be used to shut down technical innovation and to censor websites that provide platforms for personal creative expression."

Media companies, manufacturers of counterfeited goods from clothing to pharmaceuticals, and law enforcement agencies support the efforts of SOPA. They are frustrated by the often futile efforts to reach infringers operating flagrantly offshore. These companies provide vehicles for ongoing intellectual property theft. With no method of tying the assets to individuals and assets in the United States, they operate with impunity.

SOPA is drafted to address these issues. The first of the SOPA operative provisions extends the attorney general's ability to seize foreign Internet sites on the same basis the attorney general now has to seize domestic sites. While this may have significant international law implications, from an intellectual property standpoint, this serves to extend the powers provided in the PRO-IP Act to websites foreign as well as domestic. So long as these sites serve U.S. customers sufficiently to satisfy the jurisdictional requirements, the foreign sites would be subject to U.S. law for interactions with U.S. customers.

Even more striking are SOPA's remedies. Within five days of a court order, domestic ISPs "shall take technically feasible and reasonable measures designed to prevent access by its subscribers located within the United States to the foreign infringing site (or portion thereof) that is subject to the order. . . ." The provision, therefore, en-

ables a district court to shut off access to a particular URL. The ISPs are not parties to the action. Similarly, the court order would require search engine providers such as Google, Microsoft, and Yahoo to exclude the web address of such sites.

To cut off the financial transactions with these piratical sites, SOPA requires financial services providers such as Visa, MasterCard, and PayPal to stop conducting transactions with the sites pursuant to a court order. This technique provided an effective economic hit to the Wikileaks following the organization's publication of U.S. State Department communiqués and its threatened release of confidential bank records. While the actions of these financial service providers were consistent with their terms of service provisions that bar the use of the payments for illegal activities, the response to Wikileaks was troubling because the organization was never charged with any criminal wrongdoing. This situation set a very public precedent for the financial service company making the determination of illegal activity and responding accordingly.

The attorney general also has authority to bring an action for injunctive relief against any ISP, financial service provider, or Internet advertisement service that fails to take action, if it is knowingly and willingly serving the banned site. The proposed legislation limits this relief to injunctive relief only with no private cause of action, though presumably the court has civil and criminal contempt powers over any party that fails to follow its order.

While the law extends the PRO-IP Act in certain respects, it also has a rather novel reinvention of online "market-based" enforcement. Section 103 provides a two-step process that allows "an intellectual property right holder" (meaning a copyright or trademark owner) that believes itself harmed by an Internet site "dedicated to theft of U.S. property" to seek termination of that sites advertising and financial services.

The rights holder first notifies the site's payment network providers or Internet advertisement service that the rights holder believes the site is dedicated to infringement. Evidently the congressional

expectation is that for many piratical sites, the owners will be unwilling to identify themselves, so the particular site will immediately lose its payment and advertising service providers. If the site files the counter-notice, then the rights holder can continue its action against that site with much improved information to establish personal jurisdiction.

The actual language of section 103 is quite convoluted and its concept is new to intellectual property law. Unlike the provisions involving the attorney general, the market-based responses have the processes inverted, triggering the cut-off of financial services and advertising before any adjudication takes place. While there have been objections among critics of earlier legislation regarding websites being blocked by court order prior to a final judgment, SOPA goes significantly further, choking the business needs of the site before a court action is even filed.

In the House Judiciary Committee's fact sheet, the proposed process is defended as reasonable because "[t]hese are websites that are actually being used and marketed to facilitate theft, not websites or other technologies that could simply have the potential of being misused." While this may prove to be true, the process for this determination takes place after the relationships with the financial services company and advertising company have been affected.

Undoubtedly the power to throttle back the violations of copyright and trademark theft through control over the piratical sites' advertising and economic tools will prove effective. But even recognizing that litigation is more costly than a notice-and-take-down regime, such interference should only come after a court order rather than through immunity and self-help.

Presumably, the provision is built upon the logic and effectiveness of the notice-and-take-down provisions of section 512 of the Digital Millennium Copyright Act. Section 512 trades off potential direct and secondary copyright liability for immunity so long as the publisher of the copyrighted work takes reasonable steps to respond to proper notice from a copyright holder that believes its work

has been posted by a third party without authorization. Advertising services and payment services, however, have no direct copyright or trademark infringement liability and rather tenuous risk of secondary liability. Most have little ability to gain knowledge of potential copyright or trademark infringements until notice of infringement is provided. While such participants can sometimes be involved in inducing infringement or having sufficient knowledge and material participation of a direct infringer's activities, the new proposal balances a significant affirmative duty against a rather rare and remote liability risk.

In addition, the proposed legislation adds additional immunity for ISPs, Internet search engines, domain name registries, and registrars that follow comparable procedures. In essence, it incentivizes each of the Internet intermediaries to move to a voluntary notice-and-take-down system against alleged infringement sites.

Technology companies largely oppose SOPA because the obligations of enforcement and the newly created notice-and-take-down provisions will add to their duties and overhead, with potentially significant demands on their operations. The new requirements place them as the intermediaries of not only technical aspects of the Internet but also the financial and quality assurance aspects.

The PROTECT-IP Act has many of the same conceptual goals as SOPA, though drafted with less detailed provisions. At the same time, however, the PROTECT-IP Act is arguably narrower in its definition of sites subject to the law. The definition of infringing sites in each proposal has slightly different contours. The PROTECT-IP Act references provisions of the Copyright and Trademark Acts while SOPA references provisions of the criminal intellectual property provisions of Title 18. As a result, each definition has attributes that may result in it being overly inclusive for some activities while under-inclusive for others.

The most significant difference between the two proposals aside from the technical language is the notice-and-takedown provisions for financial service providers

and Internet advertising services. The PROTECT-IP Act is primarily focused on actions by the attorney general, with a much narrower provision enabling rights holders to bring in rem actions against domain names and by extension registries and registrars. It does not introduce this new form of intermediary self-regulation of Internet content.

Undoubtedly there remains significant intellectual property theft, but recent data suggests some hope that the existing efforts are starting to pay dividends. According to a recent study by the American Assembly of Columbia University, some interesting characteristics of the public are emerging:

- Piracy is common. Some 46 percent of adults have bought, copied, or downloaded unauthorized music, TV shows or movies. These practices correlate strongly with youth and moderately with higher incomes. Among 18–29 year olds, 70 percent have acquired music or video files this way.
- Large-scale digital piracy is rare, limited to 2 percent of adults for music (>1,000 music files in collection and most or all copied or downloaded for free) and 1 percent for film (>100 files, most or all from copying or downloading).
- Legal media services can displace piracy. Of the 30 percent of Americans who have pirated digital music files, 46 percent indicated that they now do so less because of the emergence of low-cost legal streaming services. Among TV/movie pirates, 40 percent.

An interesting aspect of the study addresses the public perception on adjudication. As the study explains, "Americans have relatively clear views about what constitutes due process in such matters, and it involves courts (54 percent) rather than adjudication by private companies." While a majority believes court adjudication is required, only 15 percent supported ISP based decision making and "only 18 percent percent say the music companies and movie studios should make that decision."

One other debate surrounding the proposed legislation should be noted. In a letter to the Senate Judiciary Committee regarding an earlier version of PROTECT-

IP Act, longtime Internet security advocate Kathryn Kleiman, Director of Policy for the Public Interest Registry wrote how the domain name redirection protocol "breaks the Internet." It doesn't.

What Kleiman explained in her letter to the committee was that rerouting web pages around the proper domain name server (DNS) authentication is presently a security issue being addressed by ICANN and other international Internet bodies focusing on security. The technique is used to conduct phishing, denial of service, and man-in-the-middle attacks on Internet systems. As a result, there have been steps to require authenticated DNS systems as an essential part of improved Internet security. Since the traffic redirected by court order would be sent to sites have the same attributes as phishing sites, the effect of the legislation would be to frustrate the implementation of these new security protocols.

In this context, the disruption to the Internet caused by mandatory site redirection is a legitimate concern. It presently occurs in states promoting a "local" internet such as China, but the redirection is subject to substantial international criticism. Many other analysts have raised concerns that since the techniques for users to redirect around U.S. DNS systems to offshore systems are not terribly difficult, it will drive some of the public towards these less secure systems. Such users—and any family members or others sharing their computers—would then be vulnerable to additional security problems raised by non-authenticated web surfing routed through DNS servers owned by the infringers themselves.

The analysis here emphasizes that the unintended consequence of better enforcement will be a population of less secure networked computers and greater overall vulnerability to systematic criminal behavior. At a minimum, the potential harm should be carefully studied. If these problems do develop, it will be difficult to undue such harm by subsequent amendments to the laws or through technical solutions.

It is likely the controversy surrounding SOPA and the strong positions taken by the stakeholders will result in significant ongoing debate. Nonetheless, the concerns over

piracy have not lessened. The growing success of some online copyright markets does not address the continued piracy nor does it provide relief from trademark infringement or dangerous pharmaceutical fraud.

The process for determining the best method of promoting innovation and rewarding creativity will continue. Hopefully, the discussion of SOPA will add transparency and understanding for the public on the best method of achieving these common goals.

Jon M. Garon is director, NKU Chase Law & Informatics Institute and professor of law, Salmon P. Chase College of Law, Northern Kentucky University.

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Business Interests Under Attack in Cyberspace: Is International Regulation the Right Response?

By [Henry L. Judy](#) and [David Satola](#)

Recent cyber-incidents targeting economic and business interests have turned up the heat on the debate roiling around the issue of whether there should be international legal instruments to regulate various aspects of the Internet, such as cyber-security, permissible content, and intellectual property rights. The debate ranges from technical to economic to human rights issues. As the debate is widely reported, there seem to be two very general camps emerging at the international level: one in favor of state-led international frameworks, sponsored most recently by China and Russia; and the other favoring a more libertarian view, generally comprising Western democracies, including the United States. While the United States argues in favor of a more *laissez faire*, multi-stakeholder approach at the international level, it is pursuing legal and regulatory approaches at the national level, particularly with respect to cyber-security. In terms of business and economic interests on the Internet, recent debates concerning cyber espionage is a case-in-point providing a revealing look into this ongoing debate.

"Multi-stakeholderism" is a shorthand reference to multi-stakeholder Internet governance or the multi-stakeholder model which can be described as a more "bottoms-up" approach to Internet Governance, in which governments, private companies, civil society, the technical com-

munity and other independent organizations all have roles to play but in which no single entity operates without checks and balances. The model is more directly representative and at the same time gives rise to tensions among the various parties.

More, importantly, however, the positioning of these two "opposing" camps in terms of the use of international legal instruments is a bit misleading. No one could deny either that more and better international cooperation is needed (although there are questions of where and led by whom) or that nation-states will exercise their sovereign rights to take measures to ensure and protect their interests. Rather, as further developed below, the fundamental issues involve the basic principles and values on which any international legal instruments would be based.

Threats in Cyberspace

Cyber-attacks on U.S. business interests, for example—emanating from both governmental and non-governmental sources—are on the rise and represent a "persistent threat to US economic security," according to a recent report of the U.S. Office of the National Counterintelligence Executive (ONCIX). The report, titled *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace* and issued to Congress in October 2011 states:

Foreign economic collection and industrial espionage against the United

States represent significant and growing threats to the nation's prosperity and security. Cyberspace—where most business activity and development of new ideas now takes place—amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect.

The ONCIX report specifically identifies China as a "persistent collector" of US economic data citing numerous computer network intrusions originating from IP addresses in China. The report also accuses Russia of using highly sophisticated means to obtain US economic information with the aim of diversifying Russia's heavily natural resource-dependent economy.

An International Response?

Perhaps not so ironically, the ONCIX report came out shortly after the permanent representatives to the UN of China, Russia, as well as Tajikistan and Uzbekistan, jointly submitted a draft resolution on an "International Code of Conduct for Information Security" to the UN's General Assembly in September, 2011. Adherence to the Code of Conduct would be voluntary and open to all States. It also calls for "international deliberations within the UN framework on . . . an international code, with the aim of achieving the earliest possible consensus on international norms and rules. . . ."

The 12-point Code of Conduct—some two-and-a-half pages long—provides, among other things that states adhering to the Code of Conduct would pledge:

- “Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies;”
- “To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment; . . .”
- “To reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage;”
- “To fully respect rights and freedom in information space, including rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulations;”
- “To promote the establishment of a multilateral, transparent and democratic international Internet management system to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet; . . .”

There are a number of issues with this Code of Conduct. First, as cyber-security blogger, Jeffrey Carr, has pointed out, the Code of Conduct does not follow international best practice of cross-border law enforcement as one of the most effective strategies for combating cyber attacks. Instead, he says, the Code focuses on the territorial integrity and the sovereign right

of states to protect their own information space. Second, the wording of the Code of Conduct also incorporates by implication a number of basic public international law concepts on which there is no consensus. One of these is that nation states may adopt public policy (*ordre public*) exceptions to internationally accepted human rights norms without also giving full weight to interpretive principles of predictability, transparency, legitimacy, necessity, proportionality and independence. Because it is unclear what sort of obligations would be imposed on states to “. . . cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks and *in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries’ political, economic and social stability.* . . .” (emphasis supplied), a severe, secretive and random national censorship regime would be consistent, on a verbal level, with the Code of Conduct. Finally, although it is unclear what the phrase might mean, the Code of Conduct also assumes that an “international Internet management system” is a desirable goal. This is a sharply contended proposition on several levels, ranging from the long-standing efforts of the International Telecommunication Union to have a role in the management of the Domain Name System to efforts of some countries to “manage” the permissible content of Internet transmissions from outside their borders.

The Code also assumes that “policy authority for Internet-related public issues is the sovereign right of States.” However, many states recognize that international norms place important limitations of state sovereignty with respect to crafting international responses to critical issues arising on the Internet. Take “net neutrality” for example. In the lead up to the UN’s Sixth Annual Internet Governance Forum in September 2011, the 43 member Council of Europe (CoE) announced the adoption by its Committee of Ministers of two recommendations and two declarations calling, inter alia, on CoE member states to take action to protect on-line freedom

of speech, even in the face of national security responses to cyber threats. Of particular interest is the statement on the link between net neutrality and human rights, contained in the Declaration of Internet Governance Principles. While avoiding the term “net neutrality,” which was used in earlier draft versions of the Declaration, Principle 9, titled “Open Network” provides:

Users should have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice. Traffic management measures which have an impact on the enjoyment of fundamental rights and freedoms, in particular the right to freedom of expression and to impart and receive information regardless of frontiers, as well as the right to respect for private life, must meet the requirements of international law on the protection of freedom of expression and access to information, and the right to respect for private life.

It must also be recognized that in many substantive areas governing behavior on the Internet, international legal instruments already apply. These include, most notably, the CoE’s Convention against Cybercrime (or Budapest Convention), a recognized international standard in the area of the fight against cybercrime, and to which the United States is a member. In the area of recognizing the human right of freedom of expression, Article 19 of the UN Universal Declaration on Human Rights and Article 19 of the UN Covenant on Civil and Political Rights preserve the right to receive and impart information and ideas without interference and regardless of medium and regardless of frontiers.

In addition to the basic net neutrality example, it is important to recognize that there is a tension between the “sovereign right of States” and the concept of multi-stakeholder governance as a key aspect of Internet Governance generally. If private companies, civil society, the technical community and other independent organizations all have a role to play, then the

role of states is thereby circumscribed. In addition, the concept of multi-stakeholder governance should be considered an intrusion in the traditional roles played by nation states if it is the case that the concept is strongly supported by states. In that regard the United States has taken a clear position. In May of 2011 the White House released its “International Strategy for Cyberspace” which stated as among its basic principles:

- “Upholding Fundamental Freedoms: States must respect fundamental freedoms of expression and association, online as well as off.”
- “Multi-stakeholder Governance: Internet governance efforts must not be limited to governments, but should include all appropriate stakeholders.”

On June 28 and 29, 2011 the Organisation for Economic Co-operation and Development held a High Level Meeting in Paris on the subject: “The Internet Economy: Creating Innovation and Growth.” The participants underlined the need to maintain the open, decentralized design of the Internet and emphasized that the multi-stakeholder approach has been key to the Internet’s rapid growth and impact and to the maintenance of freedom of expression and communication. In addition, the G-8 held its 2011 Summit on May 26–27, 2011 and at the end issued a declaration containing a comprehensive statement of policy on the Internet that touched on nearly every policy issue. The declaration was clear in its support of the multi-stakeholder model. Hence, the issue, once again, is not ‘international’ versus ‘national.’ The more basic question is presented of what is the role of the nation state.

In terms of cyber-security, what is the proper response to the ever evolving sophistication of these threats? More regulation? At the international level? At the national level? Not at the international level according to Assistant Secretary of State Michael Posner who addressed the Silicon Valley Human Rights Conference in late October 2011. Posner pointed out one of the soft-underbelly-features of the Arab Spring. The use of social media that

gave rise to the popular revolts, “brought home [to repressive governments] the power of the Internet.” He went on to say that “[t]oday we face a series of challenges at the intersection of human rights, connected technologies, business, and government. It’s a busy intersection— and a lot of people want to put up traffic lights.” He continued in his address to say that a system that shifted away from multi-stakeholder focus towards “a system dominated by centralized government control . . . [is] [n]ot a good idea.” On the military side, U.S. General Keith Alexander, head of U.S. Cyber Command, reacted to the draft UN resolution suggesting that regulation was perhaps not the answer. “I’m not for regulating per se,” Gen. Alexander said.

U.S. Efforts

So while there is resistance to regulate at the international level, there is at the same time, growing attention being paid to bolstering the U.S. legal framework affecting cyber-security. Indeed, cyber-security, as it affects U.S. business interests, has been on the radar screen of the U.S. government for years. In May 2009, the White House issued a review, titled “Cyberspace Policy Review,” to assess U.S. policies and structures for cyber-security. The document presents a very sobering assessment:

The architecture of the Nation’s digital infrastructure, based largely upon the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cyber-crime and state-sponsored intrusions and operations. Our digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information. Other intrusions threaten to damage portions of our critical infrastructure. These and other risks have the potential to undermine the Nation’s confidence in the information systems that underlie our economic and national security interests.

The Federal government is not organized to address this growing problem effectively now or in the future.

In May 2011, the White House sent to Congress its legislative plans for improving cyber-security for the country’s critical infrastructure, for the federal government’s own networks and computers, and for the population generally (White House Proposal). And in October, 2011, the White House issued an executive order addressing information security and data breach rules.

In Congress, dozens of cyber-related bills have been introduced in both the current session (112th) and in the previous session, reflecting a growing concern over cyber-security. The administration proposal addresses in one way or the other nearly all of the key variables in that body of proposals and can be used as an outline of the main issues. The administration proposal includes:

1. Federal data breach reporting legislation;
2. New and increased penalties for cyber-criminals, the application of the Racketeering Influenced and Corrupt Organizations Act to cyber crimes and setting mandatory minimums for cyber intrusions into critical infrastructure.
3. A framework within which businesses, states, and local governments can request and receive federal government assistance from chiefly the Department of Homeland Security for repairing damage done by cyber-intrusions and attacks and for advice on building better defenses.
4. Critical Infrastructure Cybersecurity Plans. The Nation’s critical infrastructure, such as the electricity grid and financial sector, is vital to supporting the basics of life in America. Market forces are pushing infrastructure operators to put their infrastructure online, which enables them to remotely manage the infrastructure and increases

their efficiency. However, when our infrastructure is online, it is also vulnerable to cyber attacks that could cripple essential services.

Here is where the varying positions of countries in these debates can appear a bit confusing. The U.S. response could be characterized as being exactly the exercise of sovereign rights over territorial integrity that was called for in the draft UN resolution. The various U.S. initiatives seem to support a U.S.-centric effort and exercise of U.S. sovereign rights to ensure that the security and integrity of U.S. interests in cyberspace are protected. On one level, this apparent inconsistency is no more than the constant tensions within any society between the demands of security and the demands of freedom. On another level, it is quite another thing for international instruments to be adopted that have the effect of legitimating on a global level any security regime that a nation state chooses to adopt regardless of long-standing international norms, properly interpreted.

Putting aside the question of whether there should be “international norms” as suggested in the draft UN resolution, and whether criticism of international Internet regulation can be easily reconciled with the efforts at strengthening national sovereignty (even by the United States) in cyber-space, laws alone will not do the trick, even at the national level.

The ONCIX Report also highlights what can be done beyond developing the legal framework, calling for improved collaboration among the intelligence community to better understand the nature of these cyber-economic-espionage-threats as well as pointing out the responsibilities that US corporations already have with respect to reporting on and addressing corporate risks, including cyber-threats. Specifically the ONCIX Report suggests that cross functional cyber teams across an enterprise need to be in place and that corporate officers and boards need to take an interest in network security matters (citing the 2006 Delaware Supreme Court Decision in *Stone v. Ritter*, 911 A.2d 362 (Del. Supr. 2006)(building on the 1996 decision in the *Caremark* case, 698 A.2d 959 (Del.

Ch. 1996)) that directors may be liable for failures in the company’s information and reporting systems).

A Way Forward?

With existing international legal instruments already applying, it is probably a little bit disingenuous to suggest that any movement at the international level to protect businesses’ economic interests against cyber-threats is inappropriate. It is inevitable that there will be continued pressure to address these issues on the international stage. Moreover, the absence of an agreed upon framework—whatever form that might take—including a framework for sanctions, will keep open the door for cyber-safe havens. Countries not adhering to accepted international norms in the fight against cyber-security threats will become, wittingly or unwittingly, the safe havens for those perpetrating cyber-threats. Clearly, any argument against an international “regulation” would need to take account of this, and criticisms of international regulation should not be equated with criticisms of international cooperation. The key, then, will be (1) finding—and leading—international *fora* where important issues of cyber-security will be seriously tackled (but in a manner respecting the multi-stakeholder principles already recognized in the Internet governance sphere), and (2) identifying incentives for governments of all countries, even those currently accused of cyber-violations, to participate.

Henry L. Judy is of counsel at the international law firm K&L Gates LLP. David Sattola is senior counsel in the Legal Vice Presidency at the World Bank. The authors are co-chairs of the Internet Governance Task Force of the Cyberspace Law Committee of the Section of Business Law of the American Bar Association. The views presented in this article are those of the authors in their individual capacities and do not necessarily reflect the views of the organizations with which they are associated.

For more materials on the information presented in this article, please refer to the following:

Report of the U.S. Office of the National Counterintelligence Executive (ONCIX)

http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Draft Resolution on an “International Code of Conduct for Information Security”

<http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf>;

see also briefing by Russian Ministry of Foreign Affairs

Spokesman Alexander Lukashevich, September 30, 2011, at

http://www.mid.ru/brp_4.nsf/0/908E1A6F7670AC72C325791F0029CDE8

Jeffrey Carr’s Cyber-Security Blog

<http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html>

**Article 19 of the UN Universal Declaration on Human Rights and Article 19
of the UN Covenant on Civil and Political Rights**

<http://www.un.org/en/documents/udhr/> and <http://www2.ohchr.org/english/law/ccpr.htm>

These documents were one of the foundations of the CoE’s declaration on net-neutrality.

White House, “International Strategy for Cyberspace,” May 2011

[http://www.whitehouse.gov/sites/default/files/
rss_viewer/international_strategy_for_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf)

**The Organisation for Economic Co-operation and Development, High Level Meeting on
June 28 and 29, 2011, on “The Internet Economy: Creating Innovation and Growth”**

See “Communiqué on Principles for Internet Policy Making” at

<http://www.oecd.org/dataoecd/33/12/48387430.pdf>.

White House, “Cyberspace Policy Review,” May 2009

http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

**White House Executive Order Addressing Information Security and
Data Breach Rules, October 2011**

[http://www.whitehouse.gov/the-press-office/2011/10/07/
executive-order-structural-reforms-improve-security-classified-networks-](http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks-)

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

The SEC Staff's "Cybersecurity Disclosure" Guidance: Will It Help Investors or Cyber-thieves More?

By *Roland L. Trope* and *Sarah Jane Hughes*

On October 13, 2011, the SEC's Division of Corporate Finance quietly issued new guidance (Guidance) describing disclosures of cybersecurity incidents and attacks and the prevention and remediation measures that public companies (Registrants) have suffered or may suffer, and of the prevention and remediation expenses they have expended or may expend ([CF Disclosure Guidance: Topic No. 2—Cybersecurity](#)). This Guidance is not a rule or regulation or a commission interpretation. It did not appear in the *Federal Register* for comment or otherwise. Its issuance is likely to cause substantial amounts of work among Registrants and legal professionals who represent them. At the very least, the Guidance brings new attention to cybersecurity issues in Registrants' operations and disclosures.

This Guidance appears to result from an exchange of letters between Senator John D. Rockefeller IV and SEC Chairman Mary Schapiro. Senator Rockefeller's May 11, 2011, letter noted the "growing threat and the national security and economic ramifications of successful attacks against American businesses," declared it "essential" that corporate executives "know their responsibility for managing and disclosing information security risk," and requested the SEC to issue guidance "regarding the disclosure of information security risk, including material network breaches." Chairman Schapiro responded on June 6, 2011, reciting a number of dis-

closure requirements imposed on Registrants under the federal securities laws and pointing out that certain of these requirements might obligate a Registrant to make cybersecurity disclosures:

For example, Item 503(c) of Regulation S-K may require risk factor disclosure regarding a prior cyber attack, a potential cyber attack, or the effects of a cyber attack. . . . Thus, a company should consider whether cyber attacks and vulnerabilities present specific and material risks and should avoid generic risk factor disclosure that could apply to any company.

Chairman Schapiro explained, however, that she had asked the commission staff to provide her with a briefing on "current disclosure practices" and to advise her on "whether additional guidance is needed to make sure investors have access to the information they need when making their investment decisions."

The resulting Guidance lays out six aspects of disclosures that may be affected by cyber attacks and prevention and remediation expenses. However, it gives only passing attention to the trade-off inherent in making Registrants' cybersecurity risks and prevention measures more transparent. The trade-off can be summarized as follows: The more revealing a Registrant's cybersecurity disclosures become, the greater the likelihood that they will provide information useful to hackers and

competitors (Adversaries). Specifically, a Registrant's cybersecurity disclosures, which the longstanding SEC interpretations require be specific to the Registrant rather than generic, will be understood far better by a cyber Adversary, than by a potential investor, and, accordingly, more valuable to Adversaries.

The goal of this article is to arm *Business Law Today* readers with the basics about the Guidance so that they can have conversations with clients who are or are about to be Registrants, about what this new Guidance requires in responsive disclosures and revisions to disclosure controls and procedures. The article also expresses concerns that, notwithstanding the SEC's staff's expressed intentions to the contrary, the greater transparency in Registrants' post-Guidance disclosures may provide roadmaps for cyber attacks and thefts.

Reinterpreting Existing Rules

The Guidance acknowledges that "no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents," but then advises that "a number of disclosure requirements may impose an obligation on Registrants to disclose such risks and incidents." The Guidance further notes that disclosure of cybersecurity risks and cyber incidents might be required in order to "make other required disclosures . . . not misleading" when made. SEC staff also cautions that "Registrants should

review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents.” The obligations thus created pose potentially burdensome tasks for Registrants.

Adding to “Business Risk Disclosure” Requirements

Cyber risks and costs fall within the “risks and events” that may affect the accuracy, timeliness and completeness of required disclosures. The Guidance cites obligations to keep shelf registration statements up to date, the over-arching responsibility to disclose material information (pursuant to Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9), and the antifraud provisions of Securities Act Section 17(a), Exchange Act Section 10(b), and Exchange Act Rule 10b-5, in support of responsibilities to review and disclose cyber risks and incidents so that their disclosures are not misleading to investors.

Articulating Six Key Duties

The new Guidance sets forth six aspects of Registrants’ disclosure duties under the Securities Act of 1933 and the Exchange Act of 1934 and related SEC rules:

Risk Factors

To the extent that they are “among the most significant factors that make an investment in the [registrant] speculative or risky,” the Guidance requires disclosure of the risk of cyber incidents affecting the registrant. It recommends that Registrants, in determining “whether risk factor disclosure is required,” assess their own cybersecurity risks considering all “relevant information, including prior incidents, the severity and frequency of those incidents” from quantitative and qualitative perspectives, and the “costs and consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption.” Registrants also should “consider the adequacy of preventative actions taken to reduce cybersecurity risks” from the perspective of the industry in which the registrant operates, including “threatened attacks of which [the individual registrant] is cognizant.”

Risk factor disclosures should cover the nature of “material risks” and should describe how specific risks might affect the registrant as contextually as possible, avoiding risks and effects that are generic (as SEC Regulation S-K requires). The Guidance suggests “appropriate [risk factor] disclosures” as follows:

1. Discussion of aspects of the registrant’s business or operations that give rise to material cybersecurity risks and their potential costs and consequences;
2. To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
3. Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including their costs and consequences;
4. Risks related to cyber incidents that may remain undetected for an extended period; and
5. Description of the registrant’s cyber event insurance coverage.

Management’s Discussion and Analysis

Risks and incidents should be disclosed (pursuant to SEC Regulation S-K and Form 20-F, respectively) if costs and consequences of known or potential cyber incidents would constitute “a material event, trend, or uncertainty that is reasonably likely to have a material effect on results of operations, liquidity or financial condition” or to cause reports not necessarily to indicate future operating results or financial condition. Examples include: disclosure of how a theft of intellectual property would affect the registrant’s stated results of operations, or reduce revenues, or, in the absence of a loss of intellectual property, of how an event would cause a material increase in cybersecurity prevention or remediation costs, including litigation costs.

Description of Business

Registrants must disclose (again pursuant to Regulation S-K and Form 20-F, respectively) the effect of one or more

cyber incidents on its products, services, relationships with customers or suppliers, or on competitive conditions if any would materially affect any reportable segment(s) of their businesses. The staff’s example concerns knowledge of a cyber event that could affect materially a forthcoming product’s future viability.

Legal Proceedings

If a Registrant or any subsidiary has a pending legal proceeding pertaining to a cyber incident whose outcome would affect its prospects, it should disclose the proceeding(s) pursuant to Regulation S-K. For example, if a “significant amount of customer information” had been stolen, the Registrant should disclose the court, the date the action commenced, the principal parties to the action, the factual basis for the action, and relief sought.

Financial Statement Disclosures

The nature and potential severity of cyber incidents a Registrant may have can affect its financial statements in material ways according to standards adopted by Financial Accounting Standards Board (FASB). The SEC staff’s Guidance suggests a time-bifurcated analysis and disclosure:

Prior to an Incident. The FASB Accounting Standards Codification (ASC) on Internal-Use Software requires capitalization costs for cyber prevention to be disclosed.

During and Following an Incident. Disclosures during and following a cyber incident fall into four categories regulated by specific FASB guidance:

- *Customer Payments and Incentive* requires “appropriate recognition, measurement, and classification of these payments used to mitigate cyber-incident damages.”
- *Loss Contingencies* requires determination—and recognition of—liabilities from asserted and un-asserted claims such as related to warranties, breach of contract, recalls and replacement, and counter-party indemnification of remediation expenses. If these expenses and claims are probable and reason-

ably estimable, Registrants should disclose them. Additionally, the SEC Staff Guidance requires Registrants to disclose losses that are “at least reasonably possible.”

- *Risks and Uncertainties*, requires disclosures of effects of cyber incidents that would diminish future cash flows because of impairment of intangible assets such as goodwill and other customer-related intangibles including allowances for product returns, trademarks, patents, etc. Post-event estimates and subsequent reassessments enable a Registrant to explain risks or uncertainties of “a reasonably possible change” in near-term estimates that could be material to its financial statements.
- *Subsequent Events* may require disclosures if incidents, recognized or non-recognized, occur or are discovered after a balance sheet date but before the associated financial statements are issued. Financial statements should disclose “material non-recognized subsequent” events in terms of their nature and an estimate of their “financial effect, or a statement that such an estimate cannot be made.”

Disclosure Controls and Procedures

The SEC staff Guidance also requires Registrants to disclose the effectiveness of their Disclosure Controls and Procedures to the extent that they affect the Registrant’s ability to “record, process, summarize, and report” information that they should disclose in SEC filings. In addition, Registrants should evaluate and disclose deficiencies in controls and procedures if a cyber incident would cause information not to be recorded “properly” and, therefore, would render disclosures to be “ineffective.” (SEC Regulation S-K and Form 20-F.)

What Would Cybersecurity Specialists Say about this Guidance?

Cybersecurity specialists acknowledge a simple truth: attackers need to find only one gap in an enterprise’s defenses. Registrants, in contrast, must plug and seal every gap to remain protected. As a result,

cybersecurity specialists would have five concerns about the Guidance:

1. Registrants may begin complying with the Guidance cautiously, adding cyber risks to pre-existing lists of risks and describing them in terms that are too minimal and vague to be of much use to potential investors.

The Guidance creates new burdens for Registrants, the most significant of which will probably be to craft disclosures to enable a Registrant to comply with the Guidance without revealing any information of use to an Adversary. It may help Registrants to recall that division staff admits that they are mindful that “detailed disclosures could compromise cybersecurity efforts” and that “disclosures of that nature are not required under the federal securities laws.” If the staff notifies Registrants of deficiencies in their cybersecurity disclosures, many Registrants may respond by defending the deficiency as avoiding the kind of disclosure that could compromise cybersecurity and justify it further by reminding the Staff of their position that such disclosures are “not required” by federal securities laws.

2. Cautious, minimal and vague disclosures, as noted above, are likely to help Registrants’ adversaries *before* they will become useful for investors.

The Guidance likely will have the unintended consequence of encouraging increased investment in obtaining legal advice on finding the words to express cybersecurity disclosures that will satisfy the staff without informing the Adversary. If a Registrant has to choose between complying with the Guidance and sapping its cybersecurity, the choice is clear: It will avoid compromising the enterprise. The division should not have put Registrants into the bind of having to make such choices, and should not be surprised when Registrants choose to make less informative disclosures. The Staff can then object, and a Registrant can point out to the staff the risks that the staff’s comments may well have overlooked or underestimated.

3. The Guidance calls for certain kinds of information to be disclosed that, if disclosed in detail or with any significant detail or specificity, would likely under-

mine cyber security.

A closer look at the bullet point list of “risk factor” disclosures reveals a tension between the Guidance’s aims and its disclosure requirements, some of which, as explained above, would provide potentially valuable intelligence to a Registrant’s Adversary. A Registrant that, as directed, disclosed “risks related to cyber incidents that may remain undetected for an extended period” could identify itself as a vulnerable target to Adversaries. To explain such risks without highlighting them for an Adversary would appear impossible except through use of obscure and ambiguously phrased disclosures. Similar problems would arise for a Registrant trying to discuss aspects of its operations that “give rise to material cybersecurity risks”. The staff may have seriously underestimated the skills of Adversaries.

4. If a cyber attack should follow a compliant disclosure, what is the likelihood that a shareholder’s derivative suit against officers and directors would succeed?

Registrants should not be pushed by a disclosure requirement to decide between compliance with a staff interpretation and facilitating an attack on themselves that could expose not only the enterprise’s assets to damage or loss, but that could expose officers and directors to costly and wasteful lawsuits.

5. The Guidance apparently marks the beginning, not the end, of the SEC’s efforts to influence Registrants’ cybersecurity. As revealed in testimony by Robert Cook, Director, Division of Trading and Markets (TM) before the Senate Committee on Banking, Housing and Urban Affairs Subcommittee on Securities, Insurance, and Investment, on November 16, 2011,

TM plans to enhance its ARP [Automation Review Policies] reviews, with a particular focus on whether registered entities have appropriate cybersecurity measures, and is preparing recommendations for the Commission to further strengthen the ARP standards.

(<http://www.sec.gov/news/testimony/2011/ts1116rk.htm>.)

The Guidance required disclosures that

have the result of making Registrants more accountable for cybersecurity lapses and failings. The TM plans would go further and apparently set standards for registered entities for “appropriate cybersecurity measures.” In light of the unintended consequences of the Staff’s Guidance, it seems premature and ill-advised for the SEC to be considering going even further and prescribing cybersecurity standards.

Conclusion

The new cybersecurity Guidance from the SEC’s Division of Corporate Finance recognizes the centrality of technology to Registrants’ operations and profitability, the risks that cyber-attacks present to both, and the resulting relevance of cybersecurity measures. As Deputy Secretary of Defense William J. Lynn observed in “Defending a New Domain,” *Foreign Affairs* (Sept./Oct. 2010):

Modern information technology also increases the risk of industrial espionage and the theft of commercial information. . . . Every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies.

The Guidance’s requirement that a Registrant disclose specific material information concerning their cybersecurity condition, preparedness, and experience with cyber attacks may create a Hobbesian choice for Registrants: If Registrants’ disclosures contain sufficient information to be meaningful for investors, disclosures almost certainly will have to contain information of value to Adversaries seeking reconnaissance data that will facilitate a breach or enhance its ability to exploit a cyber-vulnerability. As a result, Registrants may want to ensure that they avoid disclosures that would reveal information of particular benefit to Adversaries while, at the same time, investing in measures to improve their cybersecurity, their detection of cyber attacks, and their speed of recovery from cyber incidents.

It may be that the Guidance will achieve its purpose and provide investors with

material information that, prior to its release, Registrants had been reluctant to disclose, had not believed they were obligated to disclose, and, therefore, had refrained from disclosing. It also may be that, under the obligation to disclose such information, Registrants will be motivated to improve cybersecurity in order to avoid finding themselves in the position where their experience of a cyber attack obligates them, under the Guidance, to disclose information that would make them less attractive to investors. However close the Guidance comes to achieving such results, it also may put Registrants in a double-bind. As Tom Smedinghoff, partner in the Privacy & Data Protection practice at Edwards Wildman, observes:

If a Registrant conducts a risk assessment and finds cybersecurity deficiencies that are sufficiently material to require disclosure in its SEC filings, the registrant’s legal obligations to provide ‘reasonable’ or ‘appropriate’ data security under other applicable federal or state laws will likely also require that it take appropriate steps to address those deficiencies. Thus, in some cases, disclosing cybersecurity risks may prompt inquiry regarding compliance with applicable data security laws, and may increase the risk of potential liability for failure to provide legally required security. It may well be a ‘catch-22’ for the Registrant.

Registrants and their lawyers will not know, for a while at least, what the precise consequences of the new Guidance, intended and otherwise, will be. It also may take time for the SEC staff to discover how much value investors will gain from the required cybersecurity disclosures, or whether, as we fear, the earliest beneficiaries and the ones who stand the most to gain will be Adversaries, not investors. We hope that experience under the Guidance will not meet our most pessimistic predictions, but rather will motivate appropriate additional attention to cybersecurity.

Roland L. Trope is a partner in the New York City office of Trope and Schramm, LLP, an adjunct professor in the Department of Law at the U.S. Military Academy at West Point, and serves on the Senior Advisory Board of IEEE Security & Privacy. Sarah Jane Hughes teaches commercial law, banking regulation, and privacy at the Maurer School of Law at Indiana University. Hughes has been a regular contributor to the Cyberspace Law Survey in the Business Lawyer since 2006. The views expressed in this article are solely those of the authors and have not been approved by, and should not be attributable to, the United States Military Academy at West Point, the U.S. Department of Defense, the U.S. government, the Maurer School of Law, or the trustees of Indiana University.

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Going Mobile: Are Your Company's Electronic Communications Policies Ready to Travel?

By [Kathleen M. Porter](#)

Computers have dotted office desks for decades, and the Internet and e-mail have been common workplace tools since the mid-1990s. When the Internet and e-mail were first introduced, they dramatically increased the ability to transmit information. They also created the potential for misuse and liability. Employees surfing the Internet during the work day or accessing inappropriate websites affected productivity. In litigation, e-mails produced in discovery were often embarrassing or damaging evidence against a party.

Companies adopted "electronic communications," "Internet access," or "computer use" policies to address these misuse and liability concerns arising from the use of workplace computers and e-mail. These policies communicated to employees the company's rules for proper professional and personal use of the Internet and e-mail on the company's computers and systems, and the risks of misuse. These policies also stated that the company could look at the employees' documents, e-mails, and other content created, transmitted, or stored on the company's equipment. The policies permitted the company to view an employees' Internet browsing and viewing activity on the company's equipment. These statements dispelled any expectation of privacy that an employee might have in his or her use of the company's equipment. They authorized the company to access and monitor the employee's activities while using corporate equipment and systems. The

policy also warned employees of disciplinary action if the monitoring uncovered non-productivity or misuse.

Existing Policies are Often Inadequate

Electronic communications policies are generally premised on the fact that the company owns the computer equipment and pays for the access, security, and other services. The company has broad control over what it owns and pays for, subject only to the need to give the employee appropriate notice about monitoring and access.

However, today, business is conducted not only with workplace computers, but more often with portable devices. Additionally, employees regularly access personal web-based e-mail, social media and other accounts from their work computers. Many electronic communications policies fail to address these types of equipment and technology.

For example, many policies don't address whether and how employee-owned devices may access the corporate network. Even if remote access is contemplated, the wording may relate only to home computer access. Many policies do not consider the employee's use of his or her computer to access a private web-based e-mail, social network, or other account, or access of the Internet on his or her mobile device.

With mobile devices, a company has far less control than with corporate equipment, making it even more important for the

company to have authority to access, monitor employee activity, and take appropriate action to prevent misuse or liability. While it is not as simple as amending an electronic communications policy to add the words "and mobile devices" after every use of the word "computer," with some careful thought and planning, an effective mobility policy can be created.

Case Law on the Right to Monitor

Before discussing the components of a mobility policy, it is helpful to first review how courts have interpreted electronic communications policies generally. Many U.S. courts, including the U.S. Supreme Court, have recognized the validity of computer usage policies in defining the company's authority to monitor its employees use and activity. The Court, in the *City of Ontario v. Quon*, held that a municipality's computer use, Internet, and e-mail policy determined the scope of the employee's privacy rights in text messages he sent and received on his work-issued pager. In this case, the city's policy extended to pagers. When concerns grew that the monthly texting service plan was inadequate, the city reviewed the text messages. The employee was fired when the review revealed the employee had sent and received personal texts with inappropriate content. With a government employer, the question before the Court was whether the city's access and review of the employee's text messages was an

unreasonable search and seizure in violation of the Fourth Amendment. The Court in *Quon* found that the city's computer-use policy dispelled the employee's expectation that his text messages would be private. The Court also found that the city had the right to review whether its text plan was adequate, that it did so in a limited fashion, and as such, the city's search of the text messages was reasonable. Because the search of the text messages was determined to be reasonable, the city's termination of the employee for violating the computer-use policy was upheld.

What the Court in *Quon* did not do was set parameters on an employee's privacy expectations in his or her company's technology equipment and systems, or define the limits of the company's right to access and review the employee's documents and e-mails. Additionally, the Court did not speculate on what its holding might be if the device at issue was employee-owned rather than city-owned, or if the employee rather than the city paid for the text messaging service. However, there have been several state and lower federal court cases which have examined some of these scenarios and offer some guidance, and a few of these cases are summarized below.

The court of appeals in Georgia, in *Sitton v. Print Direction*, recently upheld the firing of a sales employee working for a competing business in violation of company policy. The employee used his personal laptop at work and connected it to the company's network. While connected, he used his personal web-based e-mail account to engage in the competing business. A suspicious supervisor went into the employee's office, moved the employee's laptop mouse around, and e-mails appeared on the screen showing the competing activity. The court in *Sitton* focused on the trial court's finding that the company's computer usage policy granted the company the authority to inspect the employee's personal computer because he used it for work. The computer usage policy also told employees they should not consider "electronic mail left on or transmitted over the company's systems to be private or confidential." The appellate court concurred with the trial court's

finding that the personal e-mail account e-mails were subject to the company's review under the terms of the computer-usage policy, and could be used to show the employee violated the company's noncompete policy.

The court in *Sitton* distinguished the facts from those in *Pure Power Boot Camp v. Warrior Fitnexus Boot Camp*, a case decided in 2008 by a federal district court in New York. In *Pure Power Boot Camp*, the court barred the company from using e-mails and documents obtained from a former employee's three password-protected personal web-based e-mail accounts to show the employee stole the company's confidential information. In this case, the employee's username and password for one of his web-based accounts was stored on the company's computers, and then used by the company to access all three accounts and find the incriminating e-mails. However, the court found that the company lacked authority to use this personal information to access the web-based accounts because there was no company policy informing the employee that company computers would be monitored or that personal web-based e-mail accounts could not be accessed from the company computers. Moreover, while the username and password were stored on the company's computers, there was no evidence that the employee downloaded these particular e-mails onto the network, or even viewed these e-mails using the company's computer systems.

In barring the company's use of these e-mails to prove its case, the court in *Pure Power Boot Camp* reviewed several cases whose holdings all turned on whether the company had a policy informing employees that company computers would be monitored, and whether the policy adequately put employees on notice regarding the lack of privacy in their computer use and their e-mail and documents.

In a recent California federal district court case, *Han v. Futurewei Technologies*, the court resisted a company's initial demands to inspect a former employee's personal computing devices and external storage devices for possible misuse or theft of the company's confidential

information because there was no actual evidence of misuse or theft. The court in the case also found no evidence an employment policy had been violated by the employee. Very concerned that the inspection of the devices might expose the former employee's personal and privileged information to the company, the court instead approved a protocol whereby the former employee's expert would inspect the devices and produce a list of documents relevant to the company's discovery request. The court's decision in *Han* was based in part on the lack of an employment policy regarding storing or transferring company files onto personal devices, and in part about a concern over access to privileged information of the employee. While the court left open the possibility of revisiting its decision upon hearing evidence of misuse or theft of the company's confidential information, if the company had a computer use policy such as the one in *Sitton*, the initial outcome may have been different.

In certain limited cases, even having an electronic communications policy may not suffice. In *Stengart v. Loving Care Agency, Inc.*, the company issued a computer usage policy, notifying employees of its right to monitor use of its computers and also asserting ownership over any data on the computers. After the employee sued for discrimination, the company preserved the contents of the employee's company issued laptop and found e-mails to her lawyer sent from her employee web-based personal e-mail account. Based on the company's policy, the trial court found the company's access and use of these e-mails in the litigation to be permissible. However, the New Jersey appellate court disagreed, and reversed the trial court's decision. In doing so, the appellate court critically parsed the terms of the policy, while at the same time underscoring the need for a showing that the employee intended to waive her attorney-client privilege. The lack of a signed acknowledgement of the policy by the employee was also a factor in the appellate court's decision.

With these cases, and others like them, we are beginning to see a framework developing regarding a company's right to

monitor mobile devices, employee-owned equipment or data created or stored on an employee supplied service. With this framework, a company can develop a mobility policy that will provide employees with the ability to use mobile devices with the company's network, while safeguarding company confidential information from misuse and theft and insulating itself from liability.

Mobile Devices

A mobility policy should broadly define what constitutes a mobile device. The definition should include battery, electric, or wireless operated devices that are easily transported and designed or capable of storing, processing, or transmitting data, text or e-mail. This broad definition captures evolving equipment and would include smart phones, portable digital assistants, mini personal computers, tablets, laptops, mini-hard drives, zip, thumb and flash drives. A company could choose to limit the definition to specific manufacturers, mobile networks, devices etc., depending on a company's needs and resources.

The Role of the IT Department

Drafting an employee policy is generally done by the human resources and legal departments. In drafting a mobility policy, the Information Technology Department (IT) should play a considerable role, including establishing the standards for identifying what manufacturers, devices, models, operating platforms, mobile networks, and service plans are acceptable in the workplace and to access the company's network. IT should also define the parameters of its assistance and support to employees with devices. Both the standards and the parameters should be incorporated into the mobility policy.

For example, IT may want to provide initial activation assistance on new devices, or on-going support to existing devices. IT may want to be responsible for identifying relevant security patches and the mechanisms for employees to download them. It may want to send updates on routine issues, or just alerts if there are concerns an employee's device has been

compromised. Additionally, IT may want to impose end-of-support life dates to avoid supporting obsolete devices. As part of any employee termination, IT may want to review, and if it is company-owned, retrieve a mobile device. IT may also need to review server logs to determine whether information was downloaded or copied in violation of the company's policy.

IT may elect to outsource some or all of these functions to a third-party mobile device management (MDM) provider, including if there are limited resources or a substantial global workforce or a broad range of mobile devices to be used with the company's network.

Who Owns the Device and Pays for Services?

An initial consideration is whether the devices and the mobile network service will be company- or employee-owned or provided or both. The company should also consider whether to offer a stipend for the mobile device or the service plan, to the extent the device is to be employee-owned. Finally, the company may want to restrict the mobile network plan to certain providers. If employee-owned devices will access the company network, IT should determine what minimum security and other standards an employee-owned device must meet to have access, and define how devices will be authenticated and visible to the network.

Security

A mobility policy should address password and authentication requirements, including requirements to periodically change passwords and for the device to time-out if it is at rest for a designated period of time. The policy should also address whether there are separate or multiple log-in and password requirements to access the device, the company's network, and any personal accounts or network access. If there are log-in requirements, the policy should address whether the employee is required to log into each with each use of the device, access or account, or whether it is permitted to have the company network access open and accessible once the employee inputs the device pass-

word. The mobility policy should require the employee to securely store his or her mobile device and not leave it unattended.

With an increase in mobile malware distributed through downloaded applications, companies have a legitimate interest in preventing malware from accessing the company computer systems through devices. Although a company controls its network, its applications and software, it is not as easy to control applications and software on devices which access the corporate network. A company can condition an employee's network access on the employee's agreement to restrict the mobile device's applications and software to only those the company approves and requires.

A company may want mobile devices to have mobile filtering and security software which control the types of sites that can be accessed and applications that can be downloaded. These requirements would be included in the mobility policy. With its authority to monitor the device, the company could also monitor devices for prohibited content and for malware. An MDM provider would have access to these types of tools and could assist a company in implementing them.

Lost or Stolen Devices

Annually, thousands of mobile devices are left in taxis or in pockets of clothes at the drycleaners or otherwise lost, stolen or misplaced. Lost or stolen mobile devices containing confidential or personal information have been the cause of numerous data security breach notifications. Therefore, being able to access and wipe a lost or stolen mobile device to prevent data loss is critically important. Knowing about the loss or theft immediately is equally important and thus, a mobility policy should require employees to immediately report device loss or theft.

Even when mandated to do so, employees often delay reporting, because they believe the device will eventually be found, or they fear disciplinary action for losing the device or they don't want to lose valuable personal photos and contact information when the device is wiped and restored to factory settings. In response, some companies have actually

permitted employees to remotely wipe their device, either directly or through an MDM provider. Other companies penalize employees, by agreeing to reimburse employees for a lost or stolen device only if the mobility policy is followed. Additionally, most mobility policies permit the company to take disciplinary action if the employee fails to report or delays reporting a device loss or theft.

An MDM provider offers 24/7 coverage to respond to employees' reports of lost or stolen devices. At least one MDM provider has developed the ability to perform a partial remote wipe on the device, in order to minimize the loss of personal photos or other private data. Most importantly, an MDM provider offers expertise, training, technology, and other resources prior to the loss or theft to minimize its occurrence and reduce its effects.

Determining Eligibility for Access

Mobile devices are not typically issued to every employee or contractor. However, some companies allow every employee or contractor network access with his or her mobile device. Companies should be aware of some Fair Labor Standards Act (FLSA) issues if the employee's mobile device has network access and messages are sent to the employee's work e-mail address outside of the workplace, and outside of normal working hours. Workers who are considered non-exempt under FLSA may be considered "working" because they receive or send e-mail outside of the workplace or outside of office hours, triggering possible overtime payments. Calculating the amount of overtime is also difficult, given that messages are sent and received intermittently. Already, numerous FLSA claims have been made based on the receipt of data on mobile devices, including ones by police officers, telecommunications workers and even an employee of a famous talk-show host.

How and When May a Device be Used?

If the device is company-owned, a mobility policy would typically provide that the device is to be used for business needs, for benefit of the company, and not for the

convenience of the employee. In many cases, a company may issue a device to an employee (exempt under FLSA) because they want them to be accessible not only during business hours but also, if needed, outside of business hours.

Ironically, many companies express a preference in their mobility policy for the employee to use a landline phone if one is available. One reason for this is that a landline is still considered to be more appropriate if the subject of the call is confidential or sensitive. A landline may also be preferred if there is a concern about the strain on the company's bandwidth. For this reason and for productivity reasons, a company may want to generally restrict the amount of the employee's use of the device in the office.

Privacy—Access, Personal Data

If the device is company-owned, then the statements in the mobility policy regarding the employee's expectation of privacy should be similar to those in existing electronic communications policies. The statements are to the effect that the company is authorized to monitor the device and the activities conducted with the device, personal and professional; and the employee has no expectation of privacy in the device or in her activity while using the device.

This issue is murkier when the employee owns the device and/or pays for the mobile network service or uses it to access web-based personal e-mail or social networking accounts. To address these situations, the mobility policy should grant the company broad authority to access an employee-owned device used for work, as well as an employee's activity on the device, including an employee's web-based personal e-mail or social network account.

The mobility policy should provide that the employee understands that he or she is being permitted to access the company's network with his or her mobile device, on the express condition that the employee agrees the company has the authority to monitor the device and activity, including activity on any web-based personal e-mail or social network account. The best evidence of the employee's consent to the

company's right to monitor and access is to have the employee sign an acknowledgement or consent to the mobility policy. Many companies incorporate the mobility policy into the employee handbook or take other steps to have evidence of the employee's acceptance of this policy. Many companies also pay for or subsidize the employee's mobile network service plan, because the service is used partially for work. If the company is subsidizing the cost of the device or the service plan so that the employee has these tools for work, this should be documented.

When the company is monitoring and accessing an employee's device and content, the company should take care to limit access to only what is needed for legitimate business purposes and do so with the advice of legal counsel.

A mobility policy should also address the fact that employees will have personal or private data on their mobile devices. The policy should authorize the company to monitor and access this data for legitimate purposes. The mobility policy should require the employee to back-up her personal data on the mobile device to avoid losing it in the event the device must be wiped.

Evolving Area

It is important to recognize that use of mobile devices for work and other purposes continues to evolve, while the life cycle of particular mobile products and technology is rather short. Any mobility policy adopted by a company today should allow for regular amendments to reflect the introduction of new devices and the retirement of older models, as well as changes in technology. Additionally, the policy should allow a company's IT and HR departments to conduct initial and ongoing training, including issuing periodic updates on security, access, and other relevant issues.

A mobility policy should strive to balance the company's interest in leveraging the benefits of technology to improve productivity with the need to safeguard the company's confidential and personal information and that of its employees and customers.

Kathleen M. Porter is an intellectual property and business transactions partner at Robinson & Cole LLP in its Boston office. She is a member of the ABA Business Section's Cyberspace Committee and a certified information privacy professional (CIPP) by the International Association of Privacy Professionals.

Additional Resources

The following article outlines components of a company policy on e-mail and using the Internet.

Business Law Today

Work station or purgatory?

Steps toward a company policy on e-mail and using the Net

By Kathleen M. Porter, David Wilson, and Jacqueline Scheib
Volume 11, Number 6—July/
August 2002

TEN CONSIDERATIONS WHEN DRAFTING A MOBILITY POLICY

<p>1. Involve IT in Defining Policy Parameters</p> <ul style="list-style-type: none"> • Have IT determine permitted and supported devices, manufacturers, models, operating systems, platforms, mobile networks, etc. • Determine IT assistance for initial activation and on-going support of a device. • Establish the controls and capability for encryption, authentication, virus protection, malware, remote wipe. • Consider using a third party mobile device management tool or provider.
<p>2. Costs and Eligibility</p> <ul style="list-style-type: none"> • Determine whether company or employee-devices or a combination. • Decide whether to give allowance or stipend for employee purchase of device or service. • Keep Fair Labor Standards Act (FLSA) in mind when establishing employees/contractors eligible for a device and/or network access.
<p>3. Security</p> <ul style="list-style-type: none"> • Establish minimum security standards for devices, access, authentication. • Decide whether to permit open or require separate log-ins to access device, voicemail, e-mail, network, or Internet. • Mandate download/use of certain security or other mobile device management tools. • Permit company to monitor device for illegal content or for malware to protect company against damage if device used to access company network. • Consider adding encryption if available or a device access timeout for when device at rest. • Obligate employee to use reasonable care in handling, safeguarding, and storing device and information and systems accessible on device.
<p>4. Privacy</p> <ul style="list-style-type: none"> • For employee-owned device accessing the company network, provide restricted connectivity so that employee is authorized to connect to network only if employee agrees to limit applications, permit access, remote wipe, and audit. • Obtain permission from employee prior to network access for the company to access device, restricted connectivity, monitor activities, and remote wipe. • Develop a plan for handling employee's personal data, including creation, storage, and use.
<p>5. Device Use</p> <ul style="list-style-type: none"> • Restrict use to business needs for benefit of company, not convenience of employee; harder to do with employee owned device. • Determine whether want employee to be accessible during non-business hours if needed, and remember the rules regarding nonexempt employees under FLSA. • Place restrictions on employee's use of device while in office to limit productivity issues and pressure on company systems bandwidth.
<p>6. Access to Company Network</p> <ul style="list-style-type: none"> • Require registration of device with company in order to access network and make device visible to IT. • Require employees to provide media access control address when available for particular device. • Condition employee's access to personal web-based e-mail account (e.g., Comcast, Verizon, Gmail, Hotmail) or access social network access (e.g. LinkedIn, Twitter, Google+, Facebook) via the company's network on the employee's agreement to allow the company access to employee's account for legitimate business purposes. • Consult legal counsel prior to accessing any employee personal or social network accounts.
<p>7. Applications and Downloads</p> <ul style="list-style-type: none"> • Restrict applications and software on device to only those approved by company. • Require HTTPS only, ActiveSync. • Require mobile filtering software to control types of sites accessed and apps downloaded on device. • Determine if network services be available through syncing with a desktop or web application. • Consider how updates/upgrades to the device will be accessed and downloaded.
<p>8. Lost or Stolen Devices; Monitoring</p> <ul style="list-style-type: none"> • Require immediate reporting of lost or stolen device or unauthorized access. • Determine disciplinary action; for illegal or unauthorized activity. • Consider disciplinary action if not compliant or if delay reporting. • Provide reimbursement for stolen device only if employee follows policy. • Consider whether to allow employees to remotely wipe directly or via a third party provider (such as Mobile Me). • Understand legal prohibitions on deducting or collecting money for company-owned device if lost, stolen, or destroyed.
<p>9. Use Outside the U.S.</p> <ul style="list-style-type: none"> • Comply with U.S. export laws regarding physical or electronic transmission of controlled data outside the United States. • Check device and review policy with employees prior to overseas travel. • Understand that other jurisdictions may have different rules on mobility, e.g., privacy of personal information; required authorization to monitor, access, or remote wipe.
<p>10. Allow for Changing Technology</p> <ul style="list-style-type: none"> • Allow for amendments, updates to reflect changing technology, models, and devices. • Allow for IT and HR to issue periodic updates/alerts for security and changes, etc.

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Delaware Insider

In re OPENLANE Bolsters Omnicare and Sheds New Light on Revlon

By [Janine M. Salomone](#) and [David B. DiDonato](#)

This month we introduce a new column focusing on Delaware corporate and commercial practice. Our column will report on and analyze recent decisions from the Delaware courts. With Delaware positioned as a leading forum for resolving complex business issues, we recognize that our readership has a profound interest in developments regarding Delaware corporate and commercial law.

We will offer a fresh column every month, written by some of the leading Delaware corporate practitioners. To start things off, Janine Salomone and David DiDonato of Potter Anderson & Corroon LLP in Wilmington have provided us with an article on the *In re OPENLANE* litigation and how it relates to the *Omnicare* and *Revlon* cases.

We're excited about our new Delaware column and hope that you are too.

* * *

Since the controversial Delaware Supreme Court decision in *Omnicare v. NCS Healthcare, Inc.*, 818 A.2d 914 (Del. 2003) (*Omnicare*), corporate practitioners have debated the extent to which a target board may permissibly employ deal protection devices to effectively "lock-up" a merger transaction without violating the principles of *Omnicare*. One deal structure utilized by practitioners and believed to be legally permissible in the wake of *Omnicare* was the so-called sign-and-consent

structure in which stockholder approval of the merger agreement was obtained by written consent almost immediately after its execution, rather than through a vote at a stockholders' meeting several weeks to several months after execution of the merger agreement. In the recent Court of Chancery decision in *In re OPENLANE, Inc. S'holders Litig.*, 2011 WL 4599662 (Del. Ch. Sept. 30, 2011) (*OPENLANE*), the court confirms that the sign-and-consent structure does not violate *Omnicare*. In addition, the court held that the *OPENLANE* board conducted an adequate sales process in compliance with its *Revlon* duties to obtain the best value reasonably attainable for its stockholders despite failing to implement traditional value maximizing tools, such as conducting an auction or negotiating for a "go-shop" provision, due, in large part, to the board's "impeccable knowledge" of the company's business.

Omnicare Revisited

The Delaware Supreme Court's 2003 decision in *Omnicare* involved a rare 3-2 split of the supreme court, with the majority holding that the directors of NCS Healthcare breached their fiduciary duties by agreeing to terms with Genesis Health Ventures that completely locked-up the deal through a combination of three components. First, the merger agreement contained a "force-the-vote" provision, which required the board to submit the merger agreement with Genesis to the NCS share-

holders for a vote regardless of whether the NCS board continued to recommend the transaction. Second, the merger agreement did not include a fiduciary-out clause that would allow the NCS board to terminate the merger agreement in the event of receipt of a superior proposal by a third party. And third, two stockholders of NCS (who were also officers and directors of the company), who together held a majority of the outstanding voting power of NCS, entered into a voting agreement in which they irrevocably agreed to vote in favor of the transaction at a later stockholders meeting. After announcement of execution of the NCS-Genesis merger agreement, but before stockholder approval of the merger, Omnicare submitted a superior unconditional offer to NCS.

The Delaware Supreme Court ultimately determined that the actions of the NCS board in adopting the aforementioned deal protections should be reviewed under the enhanced judicial scrutiny standards set forth in *Unocal Corp. v. Mesa Petroleum Co.*, 493 A.2d 946 (Del. 1985) (*Unocal*), which requires a board to demonstrate that (1) it had reasonable grounds for believing a danger to corporate policy and effectiveness existed and (2) its defensive response was reasonable in relation to the threat posed. In holding that the deal protections violated the requirements set forth in *Unocal*, the court concluded that the structure collectively constituted a coercive and preclusive defensive device

that rendered the merger a “*fait accompli*” in that the arrangements made it “mathematically impossible” and “realistically unattainable” for any other proposal to succeed. Further, the court noted that the NCS board was required to negotiate for an effective fiduciary-out in light of their continued fiduciary responsibilities to the minority stockholders of the company prior to stockholder approval of the transaction. The court’s concern did not derive from any of the deal protection measures individually, but rather from the absolute lock-up created by the combination of the force-the-vote provision, the irrevocable voting agreement and the lack of a fiduciary-out, collectively.

The dissent in *Omnicare* fervently advocated for a narrow interpretation of the majority holding, and most academics and practitioners, who thereafter commented on the decision agreed. Although never readdressed by the Delaware Supreme Court, more recent Court of Chancery decisions have led many to question the continued vitality of *Omnicare*. This view emerged, in particular, after a transcript ruling in *Optima Int’l of Miami, Inc. v. WCI Steel, Inc.*, C.A. No. 3833-VCL (Del. Ch. June 27, 2008) (*Optima*), where then Vice Chancellor Lamb approved a merger in which directors signed the merger agreement and stockholders approved the merger by written consent the next day. Thus, the transaction at issue in *Optima* did not involve circumstances similar to those in *Omnicare*, in which there was a significant period of time between board approval and the stockholder vote where the board was powerless to terminate the transaction prior to the stockholder vote, or to give stockholders a meaningful opportunity to vote against the transaction after a change of board recommendation, once a superior proposal emerged. The court distinguished stockholder approval by written consent from the lock-up present in *Omnicare* and explained that nothing in the Delaware General Corporation Law (DGCL) mandates a particular time between the board’s authorization of a merger agreement and the subsequent stockholder approval. Notably, the court found the fact that the *Optima* merger

agreement permitted termination of the transaction if the requisite consents were not obtained to be an important factor in its decision. With that in mind, the court upheld the stockholder approval by written consent and stated that the stockholders acted in accordance with the statute by submitting their consents after the board signed the merger agreement.

Background of the OPENLANE-KAR Merger

OPENLANE involved a stockholder class action seeking to enjoin a proposed merger of *OPENLANE* with and into a wholly-owned subsidiary of KAR Auction Services, Inc. (KAR). The *OPENLANE* board consisted of eight directors, including the CEO and affiliates of two private equity investors in the company. The directors (or their affiliated stockholders) held or controlled beneficial ownership of approximately 60 percent of *OPENLANE*’s outstanding capital stock.

In anticipation of a significant decline in business, the board engaged a financial advisor to assist in selling the company. The financial advisor identified numerous potential financial and strategic acquirers, but the board limited its market check to three strategic buyers. The board ultimately settled on KAR and signed a merger agreement. The merger agreement required *OPENLANE* to obtain stockholder approval (through written consents) within 24 hours of execution of the agreement. Specifically, under Delaware law and the *OPENLANE* charter, the adoption of the merger agreement required the written consent of the holders of (1) a majority of the outstanding preferred stock of the company (voting together as a single class on an as converted to common stock basis) and (2) a majority of the outstanding capital stock of the company (voting together as a single class on an as converted to common stock basis)(together, the “Majority Consent”). If the Majority Consent was not obtained within 24 hours after the board executed the merger agreement, *OPENLANE* or KAR could terminate the agreement without paying a termination fee. The merger agreement also contained a condition to closing,

which was waivable by KAR, requiring that holders of at least 75 percent of *OPENLANE*’s outstanding shares (voting together as a single class on an as converted to common stock basis) execute and deliver written consents approving the merger. The board also agreed to a no-solicitation clause with no fiduciary-out and an escrow agreement that would hold part of the merger consideration for over a year to protect KAR from certain contingencies. Within 24 hours of the execution of the merger agreement, *OPENLANE* received written consents from the holders of a majority of *OPENLANE*’s shares sufficient to approve the merger. Shortly thereafter, the 75 percent consent condition was also satisfied.

Sign-and-Consent Structure Confirmed

Consistent with the holding in *Optima*, the Court of Chancery in *OPENLANE* also concluded that the sign-and-consent structure did not violate *Omnicare*. In applying *Unocal* and distinguishing the transaction in *OPENLANE* from the transaction in *Omnicare*, the court determined that the *OPENLANE*-KAR merger was not a *fait accompli*. Unlike in *Omnicare*, where stockholder voting agreements were coupled with a merger agreement that lacked a fiduciary-out permitting the board to terminate the merger agreement for a superior proposal, the no-solicitation clause in the *OPENLANE* merger agreement appeared reasonable to the court because the board could terminate the merger agreement if the company’s stockholders did not consent to the merger within 24 hours after execution. Thus, according to the court, the no-solicitation clause, which was the one defensive device employed by the *OPENLANE* board, was of “little moment” because the board could back out of the deal if the consents were not obtained in a timely manner. Further, the court rejected the argument that the combined voting power of *OPENLANE*’s directors and executive officers constituted a defensive device that impermissibly locked-up the stockholder approval. Rather, the court found that the record suggested that there was no voting agreement and that noth-

ing in the DGCL prevents stockholders from submitting their written consent to a merger soon after board approval. In light of the foregoing, the court determined that the merger agreement did not force a transaction on stockholders or “deprive[] them of the right to receive alternative offers” and characterized the transaction as “a matter of majority rule by shareholders who were under no obligation to act in any particular way.”

Although certain commentators have characterized the *OPENLANE* decision as another step toward burying *Omnicare*, the decision is consistent with *Omnicare*. *Omnicare* cautioned against completely locking up a deal for directors and stockholders before the time to vote. *Omnicare* involved a situation in which neither the board of directors nor the stockholders could accept or consider a superior proposal before the stockholder vote, and it was contractually impossible for the board to back out of the merger, even before the stockholder vote. Irrevocably locking-up a merger before stockholders have an opportunity to vote regardless of receipt of a superior proposal arguably continues to remain impermissible under *Unocal* and the principles of *Omnicare*. *OPENLANE* did not change that; rather, it illustrates an acceptable merger approval process where stockholders merely submit their consent after the board signs the merger agreement, thereby satisfying the statutory requirement of stockholder approval. Whether those stockholders decide how they will vote before submitting their consent is of no consequence, as long as they can freely exercise their ability to give their written consent when the time for stockholder approval arises. This protects the stockholders’ right to receive alternative offers before they approve the merger and falls in accordance with longstanding Delaware case law.

Despite the holding in *OPENLANE*, in determining to utilize the sign-and-consent structure and facilitating swift stockholder approval of the transaction, a target board should be confident that other superior offers do not exist or its decision to implement the sign-and-consent structure may nevertheless give rise to a

breach of the board’s fiduciary duties under *Revlon, Inc. v. MacAndrews & Forbes Holdings, Inc.*, 506 A.2d 173 (Del. 1986) (*Revlon*) despite not being a violation under *Omnicare*.

The Benefits of Impeccable Knowledge

The *OPENLANE* decision also sheds light on factors the court may consider when analyzing directors’ compliance with their fiduciary duties under *Revlon* to secure the best value reasonably attainable in a change of control transaction. Plaintiffs asserted that the *OPENLANE* board failed to undertake an adequate sales process in violation of *Revlon* by only contacting three potential acquirers, failing to perform an adequate market check, not obtaining a fairness opinion, and relying on scant financial information. After reiterating the courts’ past proclamations that a board is not bound to a single path in order to maximize shareholder value, but instead must follow a path of reasonableness leading toward that end, the court stated that “if a board fails to employ any traditional value maximization tool, such as an auction, a broad market check, or a go-shop provision, that board must possess an impeccable knowledge of the company’s business for the Court to determine that it acted reasonably.”

The court determined that “[a]lthough the Board’s decision-making process was not a model to be followed,” there was a reasonable likelihood that at trial the board would be able to demonstrate an adequate decision-making process. The court supported this determination by emphasizing the board’s yearlong-targeted-market check, serious pursuit of transactions with two legitimate strategic buyers, receipt of data on the company’s value from a financial adviser, and the potential decline in business that the company faced. Most importantly, the court found that *OPENLANE* was “one of those seemingly few corporations that is actually ‘managed by’ as opposed to ‘under the direction of’ its board of directors” and “one of those few boards that possess an impeccable knowledge of the company’s business.” In light of this impeccable knowledge, the

court accepted the board’s argument that it failed to pursue financial buyers because it knew financial buyers had no interest in *OPENLANE*, giving considerable weight to the fact that two directors were affiliated with private equity firms and would likely have known whether the company would be of interest to a financial buyer.

With respect to the reasonableness of the board’s actions in determining not to conduct an extensive market check or obtain a fairness opinion, the court noted that *OPENLANE* was a small public company and stated that while that fact does not alter the board’s core fiduciary duties, “[w]here, however, a small company is managed by a board with impeccable knowledge of the company’s business, the court may consider the size of the company in determining what is reasonable and appropriate.” In addition, the court found the fact that the board and the current officers of the company held over 68 percent of the company’s outstanding capital stock to be a “circumstance” of the merger suggesting that the directors would be motivated to get the best price reasonably available.

Although practitioners may be tempted to read the *OPENLANE* decision as providing a free pass to *OPENLANE*’s board in terms of an adequate process under *Revlon* merely because they had “impeccable knowledge” of the company’s business, the decision does not appear to be that broad. In fact, the court points to several factors that lead to the conclusion that the board undertook an adequate decision-making process (e.g., yearlong-targeted-market check, serious pursuit of alternative transactions, seeking and receiving advice from a financial advisor, and the anticipated decline in company business). Vice Chancellor Noble focused on the board’s knowledge in order to explain away plaintiffs’ contention that the board’s failure to pursue financial buyers was unreasonable. In other circumstances, a failure on the part of a target board to pursue either financial or strategic buyers may not be viewed by the court as being a reasonable decision under *Revlon* (as in *In re Netsmart Tech. Inc. Shareholders Litig.*, 924 A.2d 171, (Del. Ch. 2007)).

Thus, having a small company with an extremely knowledgeable board is merely one factor of many considered by the court when determining if directors acted reasonably.

Escrow Agreements Do Not Violate Mandatory Standard

Finally, it bears noting that the court also determined that the inclusion of the escrow agreement as part of the overall OPENLANE-KAR transaction structure did not violate any “mandatory standard” under Delaware law. The OPENLANE merger agreement contemplated an escrow arrangement pursuant to which \$26 million of the merger consideration would be held in escrow for at least 18 months to provide KAR with protection from numerous contingencies, such as its indemnification obligations to the members of the OPENLANE board and successful appraisal proceedings. The court further stated that although the escrow agreement exposed the deal price to risk, it was proper under the circumstances because it was part of the transaction, fairly disclosed to shareholders, and within the board’s decision-making authority. The decision, however, does not contain any detail regarding the mechanics of the escrow agreement itself or otherwise go into any sort of extensive analysis regarding escrows generally so the extent to which the *OPENLANE* decision will provide precedential value if the specifics of an escrow arrangement are challenged is uncertain.

Conclusion

From a practitioner’s perspective, the *OPENLANE* decision is important because it confirms that a sign-and-consent transaction structure does not violate the principles of *Omnicare*. The decision also sheds light on the impact that company size and the board’s intimate knowledge of a company’s business may have upon a court’s review of a target board’s actions in a change of control transaction. The court’s insights with respect to each of the foregoing provides helpful guidance to companies attempting to consummate

a merger successfully, validly, and in accordance with Delaware law.

Janine M. Salomone is a partner and David B. DiDonato is an associate in the Wilmington, Delaware, law firm of Potter Anderson & Corroon LLP. The views expressed are solely those of the authors and do not necessarily represent the views of the firm or its clients.

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Member Spotlight

Kathleen Hopkins: Thoughts on Keys to the Courthouse

By Suzanne I. Cohen

Our new interview feature, “Member Spotlight,” is aimed at introducing, or at least reintroducing notable members of the Business Law Section to our readers. In the coming months, we will acquaint you with a number of BLS Advisors, Fellows, Ambassadors, and Diplomats, who will share a bit about themselves and their practices, as well as their thoughts on how the Section has enhanced their careers.

We will offer an abridged version of each interview as an online article in Q&A format, accompanied by an mp3 download for members who wish to hear the entire conversation.

We start off this month’s article with an interview of **Kathleen Hopkins**, former Editor-in-Chief of *Business Law Today* and the current Co-Chair of the Business Law Fellows, Ambassadors and Diplomats Committee. Kathleen practices law in Seattle, where she and her three close friends own a boutique law firm emphasizing commercial property transactions and financings. Kathleen was in the first class of BLS Fellows

and participates in a number of the Section’s substantive and administrative committees. She chaired our Pro Bono Committee and the ABA President recently presented her with a special



service Pro Bono Award in recognition of her passionate and longstanding service to the Pro Bono Committee and her efforts to expand pro bono across the country.

She’s also served on the Section’s Executive Council and Finance Committee and chaired the Section’s Commercial Financial Services Real Estate Financing Sub-Committee. Recently completing her term on the ABA Board of Governors, Kathleen belonged to its Non-Dues Revenue Committee and Finance Committee and chaired the Investment Sub-Committee. She belongs to the ABA’s Standing Committee on Publishing Oversight, is on the *ABA Journal* Board of Editors, and holds several positions within the ABA GP’s Solo Division, including its budget officer.

Kathleen was recently elected to the American Law Institute and is also on the American College of Commercial Financial Lawyers Board of Regents. Additionally, Kathleen is representing business and property lawyers as the ABA advisor to the Uniform Laws Commission Drafting Committee for the Uniform Asset Freezing Orders Act.

We hope you enjoy our interview with Kathleen, and those that we are planning to present in the future.

* * *

BLT: How do you think the legal field has changed over the course of your career?

Kathleen: I still consider myself a new lawyer. I’ve only been practicing for 20

years, but the field has changed a bit in that time. When interviewing with law firms as a 2L, I asked whether I would have computer access or dictate everything and have to rely on my secretary to transcribe. I’d asked because my professional career began as a secretary, I typed quickly and found it frustrating to not have computer access. Today, everyone has at least one, if not two or three devices. When I started, the turnaround time included lawyers complaining about how going from telex to fax meant their clients expected them to turn things around a lot quicker—as in the same day. Now, if I don’t answer an e-mail in an hour, that’s considered inappropriate.

The other big change is how we research. I don’t know if a lot of firms bother with libraries anymore because everything is done electronically. Our turnaround time is quicker, but timing doesn’t change our malpractice liability, so we have to be just as careful and complete in our research.

Suzanne: Your combined business and legal experience complement one another. How do the two skill sets compare?

Kathleen: I earned a B.S. in Business Administration and worked in business for 10 years. My last job before law school was assistant director of HR at a university. I’d also worked at a bank and a manufacturing company. When I do transactions, I think I understand what the client wants and can draw from my litigation experience (the first seven or eight years of my career). I under-

stand that clients need to find a business solution—it may not always match the legal solution—but I need to let them know the possible fall-out and risks and that they have to make the decisions because it's their business, not mine. Another benefit is that I'm in a firm with my three best friends. Having a business background, getting the opportunity to run a small business and apply those skill sets to real life has been quite pleasurable.

BLT: Why did you decide to pursue law?

Kathleen: I had worked in university HR for several years, enjoying the business and legal mix and union negotiations. I liked working with professors who'd been arbitrators, especially in the union negotiation area, and being able to talk with the lawyers. So, after I earned my degree, I contemplated getting an MBA. In the 1980s, there was still a lot of talk about the glass ceiling. My professors suggested going to law school, which would give me a built-in business I could open on my own using my business skills. I liked this combination. I went to law school thinking I'd become a labor lawyer, and here I am a real estate transactions attorney.

BLT: Did you ever practice labor law?

Kathleen: As a summer associate, I worked with a great labor lawyer and dabbled in labor law. But I wanted to do litigation at the onset; the attorneys in my firm who went to court the most were bankruptcy litigators. Everybody else was stuck in the morass of discovery and document review but, in bankruptcy, there's no time for that. You go to motions and trials, usually within a couple months. So I ended up jumping over and doing a lot of bankruptcies. The many real estate bankruptcies piqued my interest. When I transferred to transactional practice, it made sense to segue into the area where I'd already done litigation.

BLT: Who or what inspires you, and how have your passions guided your career?

Kathleen: My husband inspires me the most. We've been married 30 years. We inspire each other to do our best, and we're both very goal-oriented. At the ABA, I work with peo-

ple on the Standing Committee on Pro Bono, and from them to the Publications Board, to the Sections and Divisions and Foreign staff, and even in Policy, the staffers inspire me because they've committed themselves to advancing our profession's growth.

Also, I work with my three best friends. I can't ask for anything better than to practice with people you implicitly trust. I enjoy their company, and we all have separate lives. We enjoy outside activities that define us in addition to working with each other. Seeing their ability to not only practice law but also enjoy different aspects of their lives keeps me focused and balanced.

BLT: You've been involved with and contributed to many different programs within the ABA such as Pro Bono, Diversity, and the Board. How has this involvement helped shape your career?

Kathleen: I was given a very special opportunity, kind of like the precious keys to the courthouse. We have a profession and a long history and, if we want to retain our independence, it's important to hone and develop our profession for excellence. More important than making gobs of money is professional integrity. I'm always honing my skill set so I'm intellectually the best I can be at what I do. Another big part of that is making sure the profession is the best it can be. It's not the best unless we give back to the community and ensure everyone has access to justice. Projects such as the Pipeline Project and opportunities within our Section (i.e., the Ambassadors Program) make sure we reflect society. We can't give everyone access to justice unless we understand where people are coming from, and we have cultural competency. ABA involvement has helped shaped my career because it makes me a better lawyer to have participated in the Association, generally, and in this Section, specifically; both for my intellect to become a good lawyer and to better understand clients' situations.

BLT: What is the most rewarding aspect of your pro bono work? What guidance can you offer to young attorneys who wish to give back to their communities?

Kathleen: Pro bono is very personal. People

need to feel comfortable in their environments. I feel comfortable when I can use my expertise to help an individual, small business, or non-profit that otherwise would go without. There's always going to be some niche and, even if it's complex tax issues, there's a non-profit that probably needs your assistance.

Young lawyers need to weave giving back into the fabric of their jobs from day one. If it's part of who you are and what you expect to do, it becomes natural and part of your expectations. You can find opportunities, including a geographic search tool, on the ABA's [Standing Committee on Pro Bono and Public Service site](#). According to an ABA survey, over 70 percent of lawyers do some pro bono work all the time. It's part of who we are and, for the ones who don't do it, realize that you can. *Business Law Today's* column—"Focusing on Pro Bono"—describes how a business lawyer folds pro bono work into their practice.

BLT: You've obviously demonstrated a dedication to the Business Law Section and the ABA. Why did you decide to get and stay involved?

Kathleen: As a young lawyer in local bar association activities, I was asked to join the state Young Lawyers Board of Trustees because they needed somebody from my county. From there, I worked through the ABA Young Lawyers Division, the state Young Lawyers and county Young Lawyers Divisions, and was the Washington Young Lawyers president. Serendipitously, at the same time, the Business Law Section decided it needed to help develop future Business Law Section leaders. The Section initiated a new program—Business Law Fellows—offering two-year fellowships to five leaders from the Young Lawyers Division. With that fellowship, I was assigned a mentor, committee (the Commercial Financial Services Committee), and a project. So there was a way to integrate me and a reason to attend meetings—where the programming caliber, people, and their openness to working with me—floored me. The ABA asked me to become the Commercial Financial Services editor, during which I met committee leaders.

I became the Pro Bono Committee vice chair. In this administrative role, I found more opportunity to move up the leadership ranks. Both the Administrative and the Substantive Law Committees were important places for me and furthered my personal and professional development.

BLT: How are you involved in developing opportunities for young lawyers in the Section and profession?

Kathleen: I was given a special and unique opportunity. Only five young lawyers got the opportunity to be Fellows each year, and it was important when finishing my term on the Board of Governors that I give back. Now I chair the committee supervising that group. We have Fellows, Ambassadors, and Diplomats who participate in two-year fellowship programs. At any given time there are approximately 20 people we're trying to groom to become future leaders to help develop the Section.

My co-chair, **Carolyn Hahn**, recently finished her fellowship and works at the FTC. One Co-Chair has more experience and contacts to help the mentee; the other is younger, has more recently experienced the program and understands recent barriers. I do my best to get young lawyers out there, set up coffee dates and lunches, bring people together and act as a sounding board.

BLT: Where do you see yourself in the next five to 10 years?

Kathleen: I take the practice of law in five-year bites. Our law firm just celebrated our tenth anniversary, and we're renewing our lease, so I plan to practice with the same friends for at least the next five years. This summer, my husband and I loved vacationing in Ireland and Germany. We're new empty nesters enjoying being able to travel off-season. I have a nice balance of work, Bar Association activities, and travel. In 10 years, I'd like to scale back the work portion and bump up the travel.

BLT: How do you think the real estate collapse in the past few years has tested the laws and lawyers who work in real estate, and what are the main lessons learned from living

and working through this tumultuous time?

Kathleen: People need to put this in perspective. In 20 years practicing law, I've seen three up-and-down real estate cycles. This time is the worst, but it's just another cycle. The problem is that because of different financing vehicles available, it permeated more aspects of our economy and impacted more people than before. During the bubble, regardless of the technology and dollars at issue, you still had to take time to do the job correctly, be very careful and not cut corners even if it meant you'd lose the project. It's so important to stand by your integrity. We see fallout where lawyers got pulled into the mess because some opinions they gave may or may not have been 100 percent accurate. If the hairs on the back of your neck stand up, trust your instincts.

BLT: How do you see the real estate law profession and the legal profession, in general, morphing in the next few years?

Kathleen: With everything going online, our profession has changed. On the east coast, people still do closings, getting together and signing documents in a room. On the west coast, they deposit documents in escrow or go to the escrow's office when they have time and sign documents. With an online filing process, the practice of law and real estate transactions accelerates.

Financing vehicles will also morph. We saw the mortgage-backed securities market collapse, and the commercial mortgage-backed securities market is much bigger than the residential one. Many of those loans are coming due. There will be interest in how we'll replace those loans as they come due and the type of financing vehicles created or how we rework the mortgage-backed securities so they're more secure and a less volatile element in the financial market. I also see more federal regulation, especially in financing vehicles. Real estate is inherently a local practice, and it's essential for me to get counsel that's practiced in the state where I have a transaction. With individual investors buying pieces of commercial debt, I think we'll see more residential market regulation.

BLT: What three essentials does every business lawyer need to know?

Kathleen: (1) Act ethically. (2) Know the limits of your knowledge. Develop a network of people with skill sets beyond your areas of expertise. (3) Distinguish between business and legal decisions. I provide legal advice and risk assessment but leave the business decisions to the business person.

BLT: How do you recharge?

Kathleen: My husband and I love to travel and experience new places. A favorite vacation is the beach. From Seattle the closest hot, sunny guaranteed beach is in Hawaii. In May we rent a condo there where we don't even have to leave to eat. I sit on the beach with my Kindle loaded with about 20 books. Now I'm reading *All the President's Men*. My other avocation is Bar Association work—like a hobby. I also like to bike and spend time with my two grown sons, Neil and Ian.

BLT: Finally, what's on your bucket list?

Kathleen: I'm finishing a book on real estate for the GP Solar Division. In addition to teaching CLE classes, I'd like to teach a business law course to undergraduate business or MBA students or work in a law school environment. My family is very athletic—some relatives run marathons; they all do triathlons. I've been trying to hike and bike more, and, hopefully, I'll be able to do more of that.

BLT: Kathleen, this has been such a pleasure. Thank you, and have a wonderful day in Seattle.

This month's interview was conducted by [Suzanne J. Cohen](#), a Chicago-based writer who specializes in business and employee communications and social media.

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Keeping Current: UCC Setting the UCC Record Straight on Mortgage Notes

By [Steven O. Weise](#)

The press is full of articles concerning residential real estate foreclosures. Sometimes questions arise in these judicial and non-judicial proceedings concerning ownership and enforcement of the notes and related mortgages. Uniform Commercial Code Articles 3 and 9 (and related definitions in Article 1) address some of the issues that have come up in these proceedings. The litigants and the courts considering these matters sometimes do not recognize the applicability of the UCC or may have difficulty applying the rules of the UCC. *See, e.g., U.S. Bank v. Ibanez*, 458 Mass. 637, 941 N.E.2d 40 (2011).

The Permanent Editorial Board for the Uniform Commercial Code has just issued a report (Report) to explain the application of UCC provisions that govern selected aspects of these matters and how those provisions apply to common fact patterns in this area. The PEB Report addresses how the UCC governs the following matters:

- Who is the person entitled to enforce a mortgage note?
- How is the transfer of a property interest (ownership or a security interest to secure an obligation) in a mortgage note accomplished?
- What effect does the transfer of a mortgage note have on the related mortgage?

- How can a person enforce a mortgage note by foreclosing non-judicially if the person does not have a recordable assignment of the mortgage?

Procedure

The PEB prepared and issued a draft Report for public comment in March 2011. The PEB received comments and prepared revisions to the Report. The final Report was issued in mid-November. It is available on the webpages of the two sponsors of the UCC, the American Law Institute (www.ali.org) and the Uniform Law Commission (www.uniformlaws.org).

During the course of the comment period, at least two courts cited the draft Report when considering issues addressed by the Report. *See In re Jackson*, 451 B.R. 24 (Bankr. E.D. Calif. 2011) and *In re Veal*, 449 B.R. 542 (9th Cir. BAP 2011). In each case the court held for the homeowner, concluding that the person seeking to enforce the particular mortgage note had not satisfied the relevant requirements of the UCC, as explained in the (draft) PEB Report.

What the Report Does Not Cover

The Report limits its discussion to selected UCC issues:

- The Report states several times that

the UCC governs the issues that it governs, but does not address issues of real property law.

- The Report sometimes refers to the UCC's use of other law in connection with the application of the UCC's rules, for example agency law. In those circumstances, the Report notes the applicability of the other law (such as agency law) but does not discuss the content of the other law. In particular, where the UCC requires "possession" of a note to create certain rights, the Report observes that both Article 3 and Article 9 (with an assist from UCC § 1-103(b)) recognize that possession of the note can occur through an agent.
- The Report's discussion of Article 3 recognizes that Article 3 applies only to "negotiable instruments" as that term is defined in Article 3; the Report observes that if a mortgage note is not a "negotiable instrument," the Report's discussion of Article 3 issues does not apply to that mortgage note.
- The Report's discussion of Article 9 issues notes that Article 9 applies to all instruments, i.e., both negotiable and non-negotiable notes. The Report does not address all issues that might arise under the UCC in this

context, such as the possible status of a holder of a mortgage note as a holder in due course of the mortgage note and the effect that that status might have on possible defenses that the maker might be able to assert.

Who is Entitled to Enforce a Mortgage Note?

Article 3 employs the concept of a “person entitled to enforce” a note to determine the person to whom the maker of the note owes its payment obligation. UCC § 3-301. That person might or might not be the owner of the note (UCC § 3-203, Comment 1), but payment to that person discharges the maker’s obligation under the note. UCC §§ 3-412 and 3-602.

A person is the person entitled to enforce the note if *any* of the following is true:

1. The person is the “holder” of the note,
2. The person is in possession of the note, which was “transferred” to that person, but the person is not a “holder” of the note, and
3. The note has been lost or destroyed (or is unavailable for other reasons) and the person who had been in possession was a person entitled to enforce the note

These alternatives for becoming the person entitled to enforce the mortgage note are satisfied (or not) as follows:

- The first alternative is satisfied only if the person (or its agent) has possession of the mortgage note and the mortgage note is payable or indorsed to that person or indorsed in blank.
- The second approach also requires that the person (or its agent) has possession of the mortgage note. If the mortgage note is not payable to the person in possession or to bearer, then the person is not a “holder.” However, if the mortgage note was

“delivered” to the person in possession “for the purpose of giving” that person the right to enforce the instrument, the second alternative applies.

- The third alternative requires proof of the elements noted above, along with the terms of the mortgage note.

Transfer of Ownership

Unlike Article 3, Article 9 applies to interests in both negotiable and non-negotiable instruments. UCC § 9-102(a)(47). Article 9 applies to both a security interest in a mortgage note to secure an obligation and to the rights of a buyer of a mortgage note. UCC § 9-109(a)(1) and (3). Article 9 thus determines the requirements for an “effective” transfer of rights in those two situations. UCC § 9-203.

The requirements for an effective transfer of ownership (in the case of a sale) or a security interest to secure an obligation (in the case of a loan secured by the mortgage note) are straightforward:

1. Value must be given—this is typically satisfied by the payment of the purchase price in the case of a sale of a mortgage note and the promise to make a loan or the advance of the loan amount in the case of a security interest to secure an obligation. UCC § 1-204.
2. The seller or person creating the security interest to secure an obligation must have “rights” in the mortgage note—this too is usually easy to satisfy.
3. Generally, the seller or person creating a security interest to secure an obligation must “authenticate” a security agreement describing the mortgage note. UCC § 9-203(b)(3) (A). Whether the agreement covers the sale of the mortgage note or a security interest to secure an obligation, the agreement sufficiently describes the mortgage note if the agreement “reasonably identifies” the mortgage note. UCC § 9-108(a). For example, a description of mort-

gage notes by “category” or “type” is sufficient. UCC § 9-108(b)(2) and (3). (An oral (or other unauthenticated) security agreement is also possible in some circumstances. UCC § 9-203(b)(3)(B)).

If these requirements are satisfied, the buyer or lender with a security interest in a mortgage note to secure an obligation obtains a property interest in the note as owner or holder of the security interest to secure an obligation.

The Mortgage Follows the Note

The law in the United States has long followed the *Mary’s Little Lamb* rule—wherever the mortgage note goes the related mortgage is sure to follow. *Restatement (Third) of Property (Mortgages)* § 5.4. UCC § 9-203(g) codifies this rule for both sales of a mortgage note and a security interest in a mortgage note to secure an obligation. Further, perfection of a security interest in the mortgage note (whether in favor of a buyer or a lender with a security interest to secure an obligation) also perfects the security interest in the buyer’s or lender’s security interest in the seller’s or borrower’s rights in the mortgage. References to a “mortgage” in UCC § 9-203(g) include other types of consensual rights in real property to secure an obligation, such as a deed of trust. UCC § 9-102(a)(55).

Getting the Mortgage in the Secured Party’s Name

To save effort and money for all concerned, often a buyer of a mortgage note or a lender with a security interest in the mortgage note to secure an obligation will not record an assignment of the mortgage in the real estate records. As Article 9 makes clear, recording an assignment is not necessary for the buyer or lender to perfect its rights in the seller’s or borrower’s rights in the mortgage.

However, if the buyer or lender wants to foreclose, it may not have and may not be able to obtain the documents necessary to record the assignment in the real estate records, which may be necessary under local real estate law. Article 9 provides a

procedure for the buyer or lender to record a document in the real estate records to reflect that assignment. UCC § 9-607(b).

Conclusion

The PEB Report describes the application of selected provisions of UCC Articles 3 and 9 to several key issues that may come up in connection with mortgage notes.

There may well be additional UCC issues or issues arising under other law that also must be resolved, but the Report should help both practitioners and courts understand many of the issues that the UCC addresses in this area.

Steven O. Weise is a partner in the Los Angeles office of Proskauer Rose LLP.

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Inside Business Law

Focus on M&A

The [Mergers and Acquisitions Committee](#) recently distributed the Fall edition of its newsletter, *Deal Points*. M&A attorneys won't want to miss the following informative articles:

- In certain merger transactions, the merger agreement provides stockholders of the target corporation with the ability to elect the form of consideration (e.g. stock, cash, or a mix of both) that each stockholder would prefer to receive in exchange for the conversion of their shares in the merger. Such transactions raise unique issues under Delaware law, including issues regarding mechanics of the election process and appraisal rights, which are explored in [this enlightening article](#).
- When drafting a merger agreement, are you improperly drafting the language appointing the stockholder representative? A typical merger agreement will provide that the representative is appointed the agent and attorney-in-fact of the stockholders. [In this article](#), learn why additional language may be necessary according to the recent Delaware Court of Chancery opinion in *Aveta Inc. v. Cavallieri*.
- Learn all about dual-class share structures and the issues that may arise for corporations with such structures in these insightful materials. [[Materials](#) | [Program Audio](#)]
- Does your practice involve cross-border M&A transactions in Canada? If so, you won't want to miss this helpful

summary of key points that attorneys should bear in mind for any M&A deal involving Canada. [[Materials](#) | [Program Audio](#)]

- Learn about Canadian and U.S. anti-trust merger reviews by regulators in these materials from the 2011 ABA Annual Meeting which include an interesting article about antitrust enforcement under the Obama administration. [[Materials](#) | [Program Audio](#)]

Legal Opinion Q&A

The [Legal Opinions Committee](#) has a listserv where subscribers can ask and answer questions related to legal opinions. Check out listserv dialogue in the latest [Legal Opinion Newsletter](#) which includes discussion on enforceability opinions on subsidiary guaranties of parent debt, taking a broad exception for the Dodd-Frank Act, reasoned opinions and other legal opinion topics.

Cyberspace Law: Disruptive Innovation

What is disruptive innovation, you ask? Disruptive innovation can be described as the introduction of a new conceptual idea or meme into an existing system that causes the system to be fundamentally altered (e.g. assembly lines, digital film, personal computers, etc.). [Previewed](#) in the [November 2011 Cyberspace Law Committee Newsletter](#), an article by Jon Garon provides an overview of disruptive innovation from examples of the past decade, identifies the underlying patterns

of change common to disruptive innovation, and highlights strategies to mitigate disruption for existing industries, while addressing the intellectual property securitization aspects to structure effective deals for both the investors and innovators.

Hedge Funds

Do you have a hedge fund as a client? If so, these materials from the 2011 ABA Annual Meeting will prove very helpful in your practice. The presentation includes tips for negotiating with sizeable investors, legal issues for customized hedge fund products and a guide to institutional investor views and preferences regarding hedge fund operational infrastructures. [[Materials](#) | [Program Audio](#)]