November 2013

- **Our Mini-Theme: Cyber-Crime, -Cars, and -Coins: Hot Topics in Cyberlaw**

- **From Victim to Victor: Corporate Crime in the Internet Era**
  More and more companies are evaluating the benefits of being a corporate crime victim, and the options that status makes available for recovery for the harm caused by perpetrators.

- **Cyberterrorism on Wheels: Are Today’s Cars Vulnerable to Attack?**
  The potential exists that a car’s computers can be hacked, leaving the car vulnerable to infection by malware. The legal implications of this technological vulnerability have yet to be adequately addressed.

- **What’s in Your Wallet? Could it be the Department of Homeland Security?**
  Homeland Security’s proposed program to stop individuals at the border and scan their payment cards, obtain information from their financial institutions, and potentially seize funds associated with the cards raises serious legal questions.

- **Big Data and Consumer Financial Information**
  Consumer transaction data is increasingly becoming a valuable commodity. This article offers an overview of how such data is collected, used, and protected.

- **The Past and Future of Bitcoins in Worldwide Commerce**
  The bitcoin is changing the landscape of virtual currency, with some hailing it as “the next great step in Internet and global currency.”

- **Regulating the Brainspray Revolution**
  There are no current laws regarding the use of technology to capture someone’s brain signals without that person’s consent, not to mention the technology that can force bodily action through brain stimulation alone.

- **Revisiting the Public Performance Right in the Battle Over Broadcast**
  The author analyzes the legal question as to whether the retransmission of a television broadcast to viewers using new technologies constitutes a public or private performance.

Departments:

- **Keeping Current: Crowdfunding: The Real Thing Is Almost Here**
  On October 23, 2013, the SEC issued its long-awaited rule proposal on crowdfunding, bringing it one step closer to fruition.

- **Delaware Insider: Delaware Law Pitfalls in IPOs**
  There are several Delaware corporate law issues to watch out for in IPOs.

- **Ethics Corner: Our New Column: and the “No Contact Rule”**
  The goal of our newest Business Law Today column is to present topics that occasionally confront lawyers, principally business lawyers, involving the ethics rules, professionalism, and civility.

- **Focusing on Pro Bono: When Lawyers Help Out**
  Good things happen when lawyers help out. They change their community, become more collegial, and have fun. When Consumer Education and Training Services (CENTS) was born in 1995, we had one goal: to improve financial literacy in our community.

**Inside Business Law**

Late October and early November saw three great annual Committee meetings, which bear review.

The LLCs, Partnerships and Unincorporated Entities Committee held the 2013 LLC Institute, featuring a keynote speech by Hon. Myron T. Steele, Chief Justice of the Delaware Supreme Court, addressing the “Growing Importance of Alternative Entities as Compared to Corporate Structures.”

The Business Bankruptcy Committee held its 2013 Annual Meeting, featuring a smorgasbord of CLE programs and in-person working committee meetings.

Finally, the Banking Law Committee held its annual meeting, presenting numerous panels that provided a multifaceted view of current trends and issues in banking law, including a panel discussion among the general counsel of the FRB, FDIC, OCC, and CFPB.
Our Mini-theme: Cyber-Crime, -Cars, and -Coins: Hot Topics in Cyberlaw

The Cyberspace Law Committee (CLC) is getting ready yet again for its annual Cyberspace Law Institute and Winter Working Meeting. This year, we will meet January 30–February 1, 2014, at the Four Seasons Hotel in Denver, Colorado, where we will have an opportunity to meet with some of the many cyberlawyers and technology professionals in the Denver–Boulder area. This vibrant technology community, once noted for its roots in the data storage and telecommunications industry, now encompassing innovators, entrepreneurs, and lawyers involved in many areas, is one of the regions where lawyers and business leaders are confronting rapidly evolving cyberlaw issues every day. With this mini-theme, we offer a series of articles on a variety of rapidly-evolving cyberlaw topics, which we will explore further at the January conference as part of our cyberlaw agenda. The range and depth of CLC’s membership is reflected in the topics covered in this mini-theme, which was curated by Professor Sarah Jane Hughes.

First, Mark Mermelstein and Mona Amer continue the Committee’s examination of criminal prosecutions of cyber-wrongs, in “From Victim to Victor: Corporate Crime in the Internet Era.”

Continuing a look at new forms of cyber-attack, Cheryl and Richard Balough focus on new venues where our cyber-assets may be vulnerable, and the ways the law addresses the various liability that may arise, in “Cyberterrorism on Wheels: Are Today’s Cars Vulnerable to Attack?”

Next, Steve Middlebrook focuses on cybersecurity, government monitoring of payments devices, and how the Department of Homeland Security exercises its authority over cross-border funds movements at our borders. His piece is titled “What’s in Your Wallet? Could it be the Department of Homeland Security?”

Turning to data issues stemming from consumer financial transactions, and how third parties use that data, Veronica McGregor’s piece addresses “Big Data and Consumer Financial Information.”

Next, looking at how the world of finance is not only spreading online but is rapidly spreading into new kinds of currency, Denis Rice provides a summary and analysis of the rapidly growing reach of the most talked-about of the new virtual currencies, bitcoins, in “The Past and Future of Bitcoins in Worldwide Commerce.”

Ted Claypoole tackles a a growing category of cyber-business, those technologies that use human brain power to run devices, and considers the potential privacy and other legal regulatory implications they present. His contribution is titled “Regulating the Brainspray Revolution.”

Our series of cyberlaw topics concludes with a useful survey of some of the still-unresolved copyright law issues raised by the growth in digital transmission of music and video. In “Revisiting the Public Performance Right in the Battle over Broadcast,” Professor Jon Garon melds his considerable knowledge of copyright law with his past experience as a professional musician.

Join us in Denver in early 2014 for a high-powered, two-day conference that will delve deeper into a host of cyberlaw topics. Attendees will also be able to hear presentations on cybersecurity and the cloud, issues raised by the proliferation of conflicts between efforts to redress defamatory speech online and the need to preserve civil liberties on the Internet, further looks at the widespread growth of virtual currency, more issues in online payments, a further look at privacy issues in the new big data businesses and in the deployment of geolocation technologies, and the most significant cyberlaw cases of 2013. We will also roll up our sleeves and jump into interactive roundtables on a variety of cyberlaw topics, and will devote the second part of the conference to break-out sessions on many of the writing and presentation projects of the Committee’s subcommittees and task forces. All these are open sessions and provide a terrific opportunity to those new to the Committee, the Section, or the ABA to get involved in some of the most significant and most current topics of the day involving the applicability of the rule of law to the ever-changing world of business and technology.

Jonathan T. Rubens
Chair, Cyberspace Law Committee

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

Business Law Today
Developments in Cyberspace Law
(Mini-theme)
November 2012

Topics in Cyberspace Law
(Mini-theme)
December 2011
From Victim to Victor: Corporate Crime in the Internet Era

By Mark Mermelstein and Mona S. Amer

Crimes such as data breach, theft of intellectual property such as trade secrets, and the sale of counterfeit goods have reached epic proportion. Currently, the estimated annual cost of global cybercrime is $100 billion, with over 1.5 million victims per day, and more than 232.4 million identities exposed per year. This year, 59 percent of ex-employees admitted to stealing company data when leaving previous jobs. In 2011, the anti-piracy consortium Business Action to Stop Counterfeiting Piracy of the International Chamber of Commerce estimated that the yearly cost of counterfeiting and piracy is $775 billion, and is expected to reach $1.7 trillion by 2015.

Just this year, more than a dozen American and international corporations, including Nasdaq, 7-Eleven Inc., and J.C. Penney Corp. suffered data breach incidents resulting in the exfiltration of more than 160 million credit and debit card numbers, causing those companies hundreds of millions of dollars in losses. Last month, it was reported that three Eli Lilly employees walked off with $55 million worth of their employer’s trade secrets that they then sent to a competing Chinese drug company. In June of this year, trademark holders including Nike, Tiffany & Co., and the four American professional sports leagues all had their trademarks violated by counterfeiters selling knock-offs over the Internet.

Each one of the companies mentioned above was the victim of a crime. Individuals typically don’t like to be perceived as victims. The same — perhaps to an even greater degree — holds true for corporations. Being a victim is unlikely to enhance a company’s reputation. Even worse, if the company’s brand (such as a bank’s), is built around keeping client assets or information confidential, admitting that one has been the victim of data breach can significantly undermine the company’s mission. However, embracing their statuses as victims of crimes is what each of the above-mentioned companies did. Why would they do this? Unless a corporation appreciates its status as a corporate crime victim, it may not be aware of all of its available options for recovery for the harm the perpetrators have caused. Consider some of the advantages of embracing being a corporate crime victim, or “CCV.” CCVs, like all other crime victims, have statutory rights. They get the benefit of having the government work for them to investigate, prosecute, restrain the liberty of, and collect money from the perpetrators. Where the perpetrator is an employee, being a CCV may allow the corporation to insulate itself from liability for a perpetrator’s acts. Oftentimes, CCVs can collect insurance proceeds from their fidelity/crime policies. While wrapping oneself in the CCV flag may not be the solution to all of the above misconduct, it is one tool in the toolbox that should be considered alongside other more commonly used tools to redress injury, such as civil litigation.

Companies that have positioned themselves as CCVs have begun to see and take advantage of its benefits. Consider the case of former Goldman Sachs director Rajat Gupta. In 2012, Gupta was prosecuted for insider trading and convicted of conspiracy and securities fraud. As a result of Gupta’s conduct, Goldman Sachs spent millions of dollars fending off actual and potential legal attacks related to its responsibility for Gupta’s conduct and otherwise facilitating Gupta’s prosecution. Goldman, long considered a Wall Street maverick, embraced the concept that it was a CCV, a victim of Gupta’s insider trading.

Although insider trading has long been considered a victimless crime, Goldman exercised its rights as a victim of Gupta’s crime to appear at Gupta’s criminal sentencing and demand restitution for the injury it suffered at Gupta’s hands — the expenditure of significant attorney’s fees. In February of this year, Gupta’s sentencing judge ordered Gupta to pay Goldman Sachs $6.2 million in restitution to reimburse Goldman Sachs for the legal fees it incurred during its internal investigation of Gupta’s conduct, as well as during its cooperation with the government’s investigation.
and prosecution of Gupta.

Pursuant to the Mandatory Victims Restitution Act (MVRA), a “victim” is defined as “a person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered. . . .” 18 USC § 3663A. Goldman was able to position itself as a CCV, fended off any suggestion that it shared liability for Gupta’s misconduct, and received a $6.2 million restitution order. For companies that find themselves involved in misconduct such as that described above, it may well be worth considering some of the advantages of being a CCV as compared to merely being a tort victim suing in civil court.

The Government Investigates the Crime

Once an alleged crime has been referred to the government, government agencies, not the victim, investigate the wrongdoing. Indeed, the government has powers and resources above and beyond those available to private sector investigators or attorneys. These include the ability to obtain search and seizure warrants, obtain grand jury and administrative subpoenas, and utilize wiretaps and other forms of electronic surveillance. The government’s ability to threaten someone’s liberty is a great way to get witnesses to talk. The government also partners with law enforcement in other countries to gain the investigatory benefits that foreign sovereign law enforcement offers. For example, in the counterfeiting case described above, U.S. Immigration and Customs Enforcement’s Homeland Security officers conducted a joint investigation with European law enforcement agencies, since the counterfeiters were operating websites both in the United States and in Europe. This joint investigation culminated in the government seizing 328 websites that the counterfeiters were using to sell the counterfeit merchandise. While civil litigants do investigate and obtain subpoenas, their ability to go undercover, typically necessary in any cyber-investigation, is constrained by attorney ethical rules. For a CCV, having this investigation done by the government on the taxpayer’s dime, as opposed to by the company itself, can save the company significant money and likely obtain results superior to what a corporate citizen or civil litigant could achieve.

The Government Locates the Criminal Wrongdoers

The government also has tools and resources to locate and arrest the responsible parties. While U.S. residents are responsible for the majority of hacker attacks on U.S. businesses, a significant number originate in eastern Europe, Germany, China, and the United Kingdom. The United States government, as part of its crime investigation, has the ability to track suspects internationally either on its own or in conjunction with local law enforcement. The government can and does routinely obtain INTERPOL warrants for the arrest of foreign nationals and extradite perpetrators from countries with which it has extradition treaties. In the hacking case referenced above, one of the foreign defendants was arrested while in the United States sightseeing and another was arrested in the Netherlands and is currently awaiting extradition.

The Government Collects from Wrongdoers

One of the government’s most powerful weapons is its asset forfeiture power. The government has the ability to seize and forfeit property of those suspected of criminal activity. This property can then be liquidated and used to provide restitution to corporate victims. For example, in the counterfeiting case described above, not only did the government seize the offending websites, it also seized more than $150,000 in proceeds that the counterfeiters received through the websites’ PayPal accounts. Those seized funds will be forfeited to the government, and then used in part to provide restitution to the various companies victimized by the crimes. While private attorneys do have some limited ability to seize assets via civil litigation, the government will typically have the element of surprise which is significant when trying to seize portable assets such as currency. The government can also use the threat of a lengthy incarceration to incentivize criminal defendants into revealing the location or and/or repatriating further funds for restitution.

Companies Can Recover Under Their Fidelity/Crime Insurance

Many corporations invest in fidelity insurance that provides coverage for crimes such as employee theft and computer fraud. Collecting under a policy like this can be a significant source of recompense for injury to the victim corporation. However, oftentimes as a prerequisite to recovery from an insurance company, many policies require that the corporation report that crime to law enforcement.

Companies Attain Rights to Restitution and Cost Recovery

The Crime Victim’s Rights Act (CVRA) affords crime victims various rights, including “[t]he right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused,” “[t]he right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding,” “[t]he right to full and timely restitution as provided in law.” 18 U.S.C. s. 3771(a)(3), (4), (6). The rights afforded under the CVRA are available to corporate entities. United States v. Dreier, 2013 U.S. Dist. LEXIS 92863 (S.D.N.Y. July 2, 2013).

Under the Mandatory Victims Restitution Act, any assets that are forfeited to the government or are turned over to the government can be used to compensate victims of certain crimes. This includes funds that are seized from the criminal defendants, like the ill-gotten gains that were seized from the counterfeiters, or assets that were purchased with illegally obtained funds.

Not only can a company receive restitution to compensate for the crime, it may also be able to recover amounts it expended on investigating the wrongdoing. Case law has been developing around the MVRA that allows companies to receive restitution from
wrongdoers. In addition to the Goldman Sachs restitution award described above, former J.P. Morgan managing director Joseph Skowron III was ordered to reimburse J.P. Morgan for the fees it incurred investigating Skowron, who was subsequently charged with securities fraud and obstruction of justice, as well as the fees the firm incurred cooperating with the SEC during its investigation. In July of this year, the Second Circuit Court of Appeals affirmed the restitution order. The advantages of being a CCV are clear: although fees spent on internal investigations will be incurred in virtually every case of insider or employee criminality, those fees are not recoverable in civil litigation.

Companies Gain an Advantage in the Public Relations Battle

In data breach cases, attorneys general often bring civil lawsuits under their consumer protection auspices, as do consumers whose private data has been exposed. When a civil lawsuit is commenced against a corporation that understands its status as a CCV and has gotten the government involved to pursue the perpetrators, the corporation can obtain an advocacy advantage by positioning itself first and foremost as the victim of a crime, and forcing the role of principal tortfeasor onto the person who committed the theft or cybercrime. By deflecting blame onto the more significant wrongdoer, the company may make itself appear more sympathetic and make the litigation more challenging to pursue. In both litigation and public relations, wearing the white hat can yield intangible benefits.

Conclusion

To be sure, there are potential downsides to admitting one’s status as a CCV and inviting the government into a corporation’s affairs. While the company controls any civil litigation it initiates, the company cannot control the government’s criminal investigation. Similarly, if the government moves forward to prosecute a case, facts embarrassing to the CCV will probably need be turned over to the government and thus the confidentiality of that information can no longer be assured. As a result, the status of a CCV and referring the matter to the government is not a panacea. For CCVs who have suffered from data breaches, counterfeiting, or employee theft, there is typically concurrent jurisdiction to proceed by way of civil litigation, criminal referral, or both. Corporations that are reticent to embrace the status of a CCV may thereby be foregoing the best avenue to redress their injuries. Adopting CCV status is an option worth considering, particularly in situations where the facts of the case will become public anyway (because, for example, a data breach statute requires consumer notification).

Mark Mermelstein and Mona S. Amer are partner and of counsel, respectively, in Orrick, Herrington, Sutcliffe LLP’s White Collar Crime and Corporate Investigations practice. In addition to criminal defense, they spend time representing corporate crime victims.
Today’s cars are controlled by complex computer systems that include millions of lines of code connected by internal networks. Cars have become computers on wheels. The potential exists that a car’s computers, like any computer system, can be hacked, leaving the car vulnerable to infection by malware. These vulnerabilities pose serious safety hazards should they be exploited nefariously. Legal implications of this technological vulnerability have yet to be adequately addressed.

Multiple Points of Entry into a Car’s Computer Systems

Cars have dozens of electronic control units (ECUs) embedded in the body, doors, dash, roof, trunk, seats, wheels, navigation equipment, and entertainment centers. Common wired networks interconnect these ECUs, which also can connect to the Internet. This architecture provides almost unlimited gateways for external hacking and infection with malware. Some entry points to a car’s ECUs require a direct, hard-wired connection, while others can be accessed wirelessly, including using Wi-Fi or RFID. Once entry is gained, a hacker can take over all of a car’s computer-controlled systems.

In Austin, Texas, a disgruntled former employee of an auto dealer hacked into the dealer’s computer system and remotely activated the vehicle immobilization system, triggering the horn and disabling the ignition system in more than 100 vehicles. This anti-theft system had been installed by the dealer as a method of addressing non-payment by customers. While the anti-theft device was connected to the car’s horn and ignition, the hacker did not take further control of the car.

Direct Entry via the OBD-II Port

All cars made after 1996 are required to have an Onboard Diagnostics connection (OBD-II) located within two feet of the steering wheel. All cars manufactured after 2008 must share the same OBD-II protocol. The OBD-II’s initial function was to monitor mandated emissions equipment. Today, the port is used to monitor and control multiple functions. Service personnel plug equipment into the port for both diagnostics and ECU programming, typically via Windows-based computers, creating at least two paths for the introduction of malware.

First, dealership computers typically connect to the Internet (and often are required by manufacturers to do so) for daily program updates. During that process, malware could be downloaded, infecting the computers. They in turn could spread the malware when connected to a car’s OBD-II port. A second pathway is hacking into the dealership’s internal wireless network. One university research team found that it was thereby possible to use the dealer’s Wi-Fi to mount an attack.

More than dealers and mechanics use the OBD-II port. Parents can connect an app to the port to remotely monitor their children’s driving, and fleet managers use apps to keep tabs on how their fleet vehicles are being driven. In addition to hackers intent on introducing malware, clever thieves can access the port to clone “smart keys” and simply drive away with a stolen car.

Remote Entry Points

The federal government also mandates that a car have an event data recorder (EDR), similar to an airplane’s black box to record data about the status and operation of a car’s systems. While historically EDR information was collected only via physical download, primarily to conduct a post-crash assessment, newer EDR systems permit data collection over remote wireless networks. The systems automatically transmit information to an emergency response center when an accident occurs. If the EDR can communicate via a wireless network to a data collection center, then malware similarly could be transmitted back to infect the EDR.

Entertainment systems, hands-free cell-phone operations, and satellite radio also

Cyberterrorism on Wheels: Are Today’s Cars Vulnerable to Attack?

By Cheryl Dancey Balough and Richard C. Balough
provide access points to introduce malware into a car’s ECUs. For example, malware could be included in a CD inserted into the car’s entertainment system. If an attacker can compromise a smartphone that uses a car’s Bluetooth, the attacker can leverage the smartphone to compromise the car’s telematics unit. Other paths to a car’s ECUs can be accessed only at short range, such as remote keyless entry. Even tire pressure monitoring systems, which use wireless communication, are vulnerable and thus can open a pathway to the entire car’s systems.

Car manufacturers are rushing to add new Wi-Fi functions as selling points. General Motors announced that for 2014 it will offer 4G LTE wireless, allowing passengers to access a Wi-Fi hot spot for use by multiple portable devices like phones and laptops. In the past two decades, car manufacturers have begun offering remote telematics systems on their vehicles, such as General Motors’ OnStar, Toyota’s SafetyConnect, and Ford’s Sync. These systems use mobile phone voice and data communication, in conjunction with GPS technology, to give drivers hands-free remote access to emergency services, vehicle diagnostics, directions, and e-mail access. These services continue to evolve and now enable security measures such as remote ignition block and remote deceleration of a stolen vehicle. Computer scientists have demonstrated the ability to hack into such cellular-based telematics systems, transmit commands to vehicles, and surreptitiously listen to interior vehicle conversations.

Total Access All of the Car’s Computer Systems

Because all of the car’s ECUs are interconnected, once an entry point is found via any ECU, a hacker can access all car systems. While the Austin, Texas, incident demonstrates the vulnerability of a car’s computer systems in a relatively benign way, not all hackers will be as restrained. Computer scientists at the University of California, San Diego, and the University of Washington conducted multiple experiments using various remote access modalities. For every vulnerability demonstrated, they could take complete control of a vehicle’s systems – both while at rest and when traveling at high speeds. In addition, by hacking a car’s computer, a thief could remotely unlock a car’s doors, turn on its engine, arrive at the car’s location, and drive off.

Even more menacing is automobile cyberterrorism, through which a terrorist could control cars via malware, using many of the same techniques for hacking into regular computers. This vulnerability could create mayhem on the roads if a hacker broke into a vehicle network and “ordered” car ignitions to turn off or brakes to engage or disengage. In 2010, the United States and Israel allegedly created the Stuxnet worm, which reportedly destroyed 1,000 centrifuges Iran used to enrich uranium by taking over the computerized systems operating the centrifuges. Stuxnet alerted critical infrastructure providers to the lack of protection from basic hacking. Automakers are no different than other infrastructure providers and are similarly vulnerable to cyberterrorism.

V2V and Self-Driving Cars

The potential vulnerability of cars to hacking will increase as vehicle-to-vehicle (V2V) and self-driving cars become available. V2V communication allows vehicles to send each other via Wi-Fi information such as location, speed, and direction of travel. Other data that may be exchanged include lateral acceleration, longitudinal acceleration, throttle position, brake status, steering angle, headline status, and the number of occupants in the vehicle.

Companies are gearing up for the V2V market. Google has been testing cars controlled solely by computers. Ford Motor Company expects to launch such cars by 2017. Two states, Nevada and California, have passed legislation allowing driverless cars on their roads. It is estimated that by 2040, self-driving cars could account for 75 percent of road traffic. At the 2013 Detroit Auto Show, Audi demonstrated a self-parking car, which one can retrieve from the garage via smartphone.

Industry and Government Addressing the Threat

One security expert estimates that the average auto maker is about 20 years behind software companies in understanding how to prevent cyberattacks. Like many computer systems, car computers previously were “air-gapped” from the Internet but are now connected via cell phones, Bluetooth, computerized diagnostic systems, and other exposed entry points. As long as the ECUs were not connected externally, the danger of introducing malware into a car was low and, as a result, the need to have sophisticated and updated security controls remained a low priority. Given today’s connections, however, control systems must be designed to thwart cyberattacks.

This very real threat has prompted both the auto industry and the government to begin taking action. General Motors has a patent application pending for remote reprogramming of vehicle flash memory using digital satellite broadcast or other wireless transmission to the vehicle, thereby closing any “air-gap” between the car’s ECUs and the Internet or any potential cyberattacker. SAE International, North America’s largest automotive trade group, formed a special committee to draft new standards for security measures in automotive electronic systems. The U.S. Department of Transportation also is revising its testing procedures for automotive electronics.

Until industry-wide standards are adopted and implemented, cars, their owners, and their passengers remain vulnerable, creating liability concerns for the automotive industry. If a malware attack were to occur, vehicle owners might be able to assert causes of action for defective design under state laws and for breach of implied warranty pursuant to the federal Magnuson-Moss Act. Most states have consumer protection laws targeted at unfair methods of competition and unfair or deceptive practices. These statutes might create a duty to disclose an objective, identifiable safety risk to consumers. California courts have found that defects in automobiles that could cause sudden or unexpected engine failure while driving pose such a risk. Evi-
dence that a defect causes car engines to shut off unexpectedly or causes individuals to stop their cars under dangerous conditions also can trigger the duty to disclose.

In a class action involving plastic coolant tubes that cracked, leaked, or otherwise failed in a car, the plaintiffs alleged that the defendants knew, reasonably should have known, or were reckless in not knowing about the coolant tube defect but failed to disclose the defect to consumers. The court found the allegations were sufficient to sustain causes of action under many state consumer protection acts. The court also found that the Magnuson-Moss Act claims required that the warranties be determined by state law, and the court conducted a state-by-state analysis, finding the allegations sufficient in some states but deficient in others.

Similarly, if a court were to find that an auto maker knew or should have known about its cars’ vulnerability to hacking and should have disclosed that vulnerability, then a consumer might have a cause of action under consumer protection laws. As for a breach of implied warranty claim, cars generally have warranties expressed in a number of years or miles. There is no specific “shrink wrap” type of agreement for the millions of lines of code in today’s cars. If a court were to find an implied warranty that runs with a car’s ECUs, then this cause of action might also exist for consumers if their cars are hacked into and controlled by malware.

Consumers whose car ECUs are compromised might alternatively sue auto makers under a defective design theory. Toyota owners took this approach after their vehicles suddenly accelerated. The court denied Toyota’s motion to dismiss finding the complaint supported a design-defect claim given that the cars “do not meet consumer expectation because they suddenly and unexpectedly accelerate and cannot be stopped upon proper application of the brake pedal, [causing] crash and injuries.” The court also denied Toyota’s motion to dismiss a count for “warning defect theory,” which allows for a cause of action even though a product is manufactured or designed flawlessly if the manufacturer later learns there is a product defect.

While auto companies may argue that the threat of a third party inserting malware into a car and taking it over is beyond their control because it is external, similar arguments in the past have been rejected. Otherwise, courts have noted, all defective designs would be characterized as external even if they are predictable. Similarly, in the case of a malware invasion through inadequately protected points of entry to a car’s systems, the threat is not just external, but predictable. By failing to protect the car’s systems from malware, the predictable consequences are potentially disastrous and car companies might be liable for defective design of the computer systems without adequate protection in light of known cyber threats.

Protected Computer Under the CFAA?

Even with the efforts of multiple groups to thwart automobile cyberterrorism and other malicious attacks on car computer systems, the past couple of decades have taught us that hackers will always try to stay a step ahead. It is important to determine whether existing laws provide viable means to address hacking into automotive computer systems as a civil cause of action or criminal offense.

If a hacker or terrorist gains access to a car’s ECUs and installs malware, that insertion would be without authorization under the Computer Fraud and Abuse Act (CFAA). The ECUs meet the CFAA’s definition of a “computer,” that is, the ECUs are high speed data processing devices performing logical, arithmetic, or storage functions. More problematic, however, is whether a car and its ECUs meet the definition of a CFAA “protected computer.” In order to qualify, the car or ECU must be a computer “which is used in or affecting interstate or foreign commerce. . . .” Cars do travel in interstate commerce, but does the computer system affect interstate commerce as defined under the CFAA? At least one court found that in order to qualify as a protected computer, a computer must be used in interstate commerce. In other words, if the computing activity at issue takes place entirely within one state, the computers are not used in interstate commerce.

Even if a car itself is not a protected computer, the pathway to hacking a car’s ECUs might involve a protected computer. If a person takes a car to a dealer for routine maintenance, a dealer’s infected diagnostic computer could introduce malware into the car through its OBD-II port. Because the dealer’s computer connects to the Internet, it is a protected computer under the CFAA. Similarly, a person may subscribe to an auto insurance company’s program that monitors car usage to reduce premiums. The insurer tracks the car’s usage in part by attaching a monitoring device to the OBD-II port. If the insurer’s computers are hacked to plant malware aimed at cars, this malware could be transferred in violation of the CFAA when the insurer’s computer connects to the insured’s car—a use in interstate commerce.

Whether or not the CFAA applies, car dealerships and insurance companies need to determine how they will address hacking. If a dealer or insurer discovers its computer system has been compromised to the point of infecting car ECUs, disclosure of the incident might not be mandated under state laws because the breach does not involve personal information. Given liability concerns, however, disclosing the security breach to car owners might be wise.

The DMCA and Protection

Assuming some software programs used to operate a car’s systems are copyrighted and automakers have taken measures to prevent access, hacking into a car might violate the Digital Millennium Copyright Act (DMCA), which prohibits circumvention of technological measures to gain access to a copyrighted work. The DMCA’s anti-circumvention provision creates a separate cause of action even when no copyright infringement exists. The Ninth Circuit found a violation of this provision in MDY Industries, LLC v. Blizzard Entertainment Inc., 629 F.3d 928 (9th Cir. 2010). However, the appellate court declined to grant
the plaintiff relief because the technology used to prevent access was not an effective access control measure. In reaching its decision, the appellate court cited a Sixth Circuit case, which found that to qualify under the DMCA, the technological measure must effectively prevent access. Therefore, a party seeking to use the DMCA to pursue the hacker of a car’s ECUs would need to show that its car has technological measures that effectively control access.

Possible Violation of the Wiretap Act

Hacking into a car’s ECUs might not by itself be a violation of the Wiretap Act, but how a hacker inserts malware into a car’s ECUs could violate the act. The Wiretap Act prohibits intentional interception of an “electronic communication,” which it defines as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12). A hacker’s interception of signals or data transmission between the ECUs within a car arguably would not affect interstate commerce. In addition, insertion of malware into a car’s internal networks through its OBD-II port, a DVD, or a USB drive connected to a mechanic’s diagnostic system without interception of data would not implicate the Wiretap Act because no interception occurs. However, if a hacker actually intercepts an electronic transmission, e.g., a diagnostic system update from a manufacturer to its dealers transmitted via the Internet, in order to insert malware into the transmission, then the hacker arguably violates the Wiretap Act.

Intercepting transmissions from a vehicle also would violate the Wiretap Act. The act excepts from coverage certain types of electronic communications, including “an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.” At least one court, however, has found that the ability for someone with specialized equipment to remotely capture data transmitted from a computer does not mean such data transmissions fall under the readily accessible exception of the act.

In an interesting twist, the Ninth Circuit found the operator of a vehicle monitoring system could not be ordered, pursuant to the Wiretap Act, to assist the Federal Bureau of Investigation (FBI) in monitoring conversations inside a car. The Company v. U.S., 349 F.3d 1132 (9th Cir. 2003). One feature of the OnStar system allows the system’s operator to open a cellular connection and listen to communications in the car. A purpose of this feature is to overhear thieves after a car is stolen to aid in the vehicle’s recovery. Upon FBI’s request, a district court issued several ex parte orders to allow eavesdropping under the Omnibus Crime Control and Safe Streets Act of 1968. The court found the monitoring service fell under the definition of the statute and required cooperation with law enforcement officials. However, when the OnStar listening feature was engaged, it disengaged other OnStar functions, including the button for automatic emergency response. On appeal, the Ninth Circuit found the lower court order invalid because it caused more than a “minimum of interference” with OnStar’s services, so OnStar could not be ordered to comply with the FBI request.

How the Wiretap Act can assist law enforcement or civilians in addressing the vulnerability of a car’s ECUs is not yet resolved.

Applicability of a Trespass to Chattel Tort Theory

A cause of action for trespass to chattel, governed by state law, might hold hackers liable for their activities. Generally, the tort requires intentionally dispossessing another of chattel, or using or intermeddling with chattel in the possession of another with resulting harm in the form of property damage or diminution of quality, condition, or value. An Illinois court found the plaintiff’s allegation of trespass to chattel by defendant’s installation of spyware on his personal computer was sufficient to withstand a motion to dismiss. Sotelo v. Direct-Revenue, LLC, 384 F. Supp. 2d 1219 (N.D. Ill. 2005). Therefore, this tort might be a valid cause of action to employ in seeking damages from a hacker.

The PATRIOT Act

The PATRIOT Act and its extension modified numerous existing laws to protect against terrorism. However, the act does not address specifically cyberterrorism via cars. The act addresses terrorist attacks and other acts of violence against mass transportation systems, which are defined as passenger vessels, railroads, intercity bus transportation, school buses, and charter and sightseeing transportation, but it does not mention private passenger vehicles or trucks. The act also added to the punishment section of the CFAA offenses that are “a threat to public health or safety,” but it did not otherwise amend the CFAA. As a result, the PATRIOT Act does not directly address car cyberterrorism.

Conclusion

Car makers are taking steps to reduce vulnerabilities to malware and cyberattacks that exist in their computers on wheels as they continue to roll out new products with even more technology. Legislatures and judges also will need to examine how today’s laws apply to damage caused when hackers or terrorists exploit these vulnerabilities. These challenges will not disappear, but they might spawn a new industry: daily antivirus software updates for cars.

Cheryl Dancey Balough is the communications co-director of the American Bar Association’s Cyberspace Law Committee and adjunct professor at Chicago-Kent College of Law. Richard C. Balough is the co-chair of the American Bar Association’s Mobile Commerce Subcommittee of the Cyberspace Law Committee. Both are founding members of Balough Law Offices, LLC, a Chicago-based law firm that represents businesses in protecting and developing their intellectual property assets.
A hot topic in the financial services industry press is news that the Department of Homeland Security (DHS) has plans to stop certain people at the border and scan the payment cards in their wallets, check the cardholder’s balances and, in certain cases, seize the funds on the card. The initiative is related to regulatory changes proposed by the Financial Crimes Enforcement Network (FinCEN), the part of Treasury that oversees anti-money laundering regulations. 76 F.R. 64049 (October 17, 2011). FinCEN requires people crossing the border to declare if they are carrying more than $10,000 in “monetary instruments.” Monetary instrument is currently defined to include cash, traveler’s checks, certain negotiable instruments, and securities. Because law enforcement has concerns that prepaid cards are being used by criminals to launder money and move it out of the country, FinCEN has proposed adding prepaid cards, but not debit or credit cards, to the list of monetary instruments that must be declared at the border.

Assessing the value of paper currency and negotiable instruments is relatively easy because the value appears on the face of the document. This is not true, however, for prepaid and other payment cards. To determine how much money is associated with a card, you must contact the financial institution that issued the card and query the current available balance. Consequently, verifying the value of a prepaid card at the border cannot be done independently by the border agent but requires the government to obtain information from the issuing financial institution.

Homeland Security has acknowledged their new program in several documents as well as in meetings with the card networks, but we still don’t know much about how it will be implemented. DHS stated in a comment letter it filed regarding the FinCEN proposal that it plans to deploy hand held devices at the border to scan debit, credit, and prepaid cards and report back information about the cardholder’s account. In addition to cards, Homeland Security has suggested the FinCEN requirements should also apply to “cell phones, key fobs, or other tangible objects” that might possibly be tied to a prepaid account. In a procurement document seeking vendors of the card scanners, the department required the devices to also be able to read Near Field Communication (NFC) chips. Cell phone makers are starting to incorporate NFC technology into their products in order to facilitate mobile payments. DHS’s NFC requirement suggests it plans on scanning mobile phones as well as payment cards in order to obtain information about travelers from their financial institutions. DHS’s plan represents an unprecedented intrusion into individual privacy that raises serious and troubling legal questions for financial service providers as well as general businesses that use cards to pay wages to employees and for other purposes. This departure from current practice seems especially unwarranted given that the program will do little to combat the illegal movement of money across borders.

The Money Laundering Risk is Small and Getting Smaller

Prepaid cards are similar to debit cards, but rather than being tied to a checking account, they draw funds from a prepaid balance placed with the issuer by the cardholder or a third party such as an employer or government agency. The cards can be used to make purchases at retailers and some also allow for access to cash at ATMs. Government and private employers have embraced prepaid cards as a way to pay benefits and wages while avoiding the expense and burden of cutting paper checks.

For a number of years, law enforcement has expressed concern that prepaid cards could be used by criminals to launder the proceeds of illegal activity and remove it from the country, although no significant cases involving prepaid cards have been prosecuted. In response, both FinCEN and banking regulators have strengthened their
rules regarding prepaid products and increased oversight of institutions that offer such products. In addition, banks, processors, and other entities involved in prepaid have significantly stepped up their anti-money laundering (AML) programs, adopting more stringent customer identification and transaction monitoring programs to prevent criminal use of their products. As a consequence, the risk potential for prepaid has been lowered significantly over the past few years. A January 2013 study by the Federal Reserve Bank of Atlanta reviewed a number of prepaid programs to evaluate the potential they could be used for money laundering and concluded: “Given both the regulatory and industry measures in place for mitigating money laundering risks associated with U.S.-issued GPR prepaid cards, these products are no longer the attractive instruments for money laundering that they once might have been.” While law enforcement may still have concerns about misuse, those fears have not materialized and the risk that prepaid cards will be used for money laundering purposes continues to decrease over time.

The Program Faces Significant Operational Issues

The FinCEN rules and DHS’s scanning program face operational hurdles which will make it difficult for them to achieve their intended goals. Lawyers familiar with how prepaid cards and mobile payments work have expressed skepticism that the FinCEN rule changes will actually detect any money laundering. A criminal who is sophisticated enough to move money out of the country using a prepaid card would be smart enough to get around the declaration requirement by copying the information from the magnetic stripe on the card to the memory of a computer, iPod, or other digital device, or by sending it over the Internet and then creating a duplicate card outside the country. Also, since DHS will be looking at balances at a single point in time, individuals could avoid detection simply by timing loads to the cards to occur after the border crossing. Ultimately, the new rule is unlikely to catch any criminals, but may very well entrap innocent law abiding citizens. The distinctions between credit, debit, and prepaid cards are not well understood by the general public and consequently we should expect the number of incorrect disclosures to be high. FinCEN’s requirement will undoubtedly result in both under and over reporting by confused cardholders. In addition, to make an accurate disclosure, the cardholder must know the exact balance on his or her card. While most prepaid programs allow cardholders to inquire about their balance through a phone call, over the Internet, or by text message, it isn’t clear that someone standing in line at the airport will always have the ability to obtain current information about his or her account. In the end, the reporting rule does not appear geared toward generating much information useful in preventing money laundering, but it may make unintentional criminals out of average citizens simply because they don’t know whether their payroll or government benefits card is technically a debit or prepaid product or that a deposit has been posted to their account since they last checked their balance.

There is even greater concern with regard to whether the Homeland Security scanning program can be successfully implemented. While the FinCEN rule would add prepaid cards but not debit cards to the list of monetary instruments that must be disclosed at the border, as noted above, it is very hard to tell the two apart. The difficulty stems in part from a settlement agreement resolving antitrust claims brought by Wal-Mart and other retailers against Visa and MasterCard, which requires that both debit and prepaid cards be labeled “debit” on their face. In re Visa Check/MasterMoney Antitrust Litigation (CV-96-5238 E.D.NY). Even well trained border agents are apt to be confused. Homeland Security seems to understand this problem, because their plan is to ignore the distinctions and scan all payment cards – prepaid, debit, and perhaps even credit – and then see what information is generated. Consequently, while on the surface DHS’s plan appears only to impact prepaid cards, its negative effects will be felt by users of all types of payment cards.

The card networks require a cardholder’s consent for most transactions, usually manifested by signing your name or entering your PIN. DHS, however, intends to submit card transactions without cardholder consent, which would violate the network rules. In order to seize the funds on the card, it appears DHS will initiate a standard point-of-sale purchase transaction which normally also requires the customer’s authorization. Presumably DHS will either have to force the cardholder to authorize the transaction with a signature or PIN or submit the transaction without permission – in either case, the transaction will not be supported by voluntary consent and thus be of dubious legality. Under Regulation E, cardholders have a right to dispute unauthorized transactions, so the traveler who has had money seized at the border may very well contact the card issuer and demand that his or her money be returned. In a case like this involving an unauthorized transaction, the card issuer would typically refund the transaction amount to the cardholder and initiate a chargeback against the merchant to recover the funds. It seems unlikely that DHS will cooperate with the chargeback process, however, and the card issuer will be left to sort out the mess and probably take the hit on the loss. Lawyers for financial service providers should be prepared to advise their clients who may find themselves in this conundrum.

It’s important to note that the card networks were built to allow cardholders to make purchases at participating merchants, not to allow the government to obtain information about its citizens. While the networks may support transactions that allow for a balance inquiry or a purchase, those transaction types were not designed for what Homeland Security wants to do and it is unclear if they will work as DHS expects. In other words, even if DHS successfully obtains financial data related to the card, that information may not mean what DHS thinks it means. Without more transparency from the government, it is not possible to determine if, or to what degree, the plan to scan cards at the border will produce mean-
The Program Will Harm Innocent People

The FinCEN reporting requirements will apply to everyone who carries a prepaid card across the border. Who are these people? One large category of prepaid users is recipients of state and federal benefits. In a 2012 report, the Federal Reserve Board found that 158 different federal, state, and local programs made approximately $100 billion in payments utilizing prepaid cards. Governments have increasingly switched to prepaid cards from checks to make benefit payments to unbanked recipients. The cards are faster, safer, and significantly cheaper, saving cash strapped agencies millions of dollars a year. The U.S. Treasury has been a leader in this area with its Direct Express card which is now used by over 4 million people to access their Social Security, VA, OPM, and other federal benefits. In addition, most states now deliver food and nutrition assistance, unemployment insurance, child support, and other government payments to recipients via prepaid cards. The DHS program will turn these millions of people into second class citizens at the border and subject them to extra rules and requirements simply because they receive Social Security benefits or some other government payment on a prepaid card.

Prepaid cards are also popular with individuals who for whatever reason cannot or choose not to open a traditional bank account. This population tends to be younger, lower income, and disproportionately comprised of African-Americans, Hispanics, and recent immigrants. The National Urban League reports that over half of African-American households are either unbanked or underbanked and that 33 percent of black Americans use reloadable prepaid cards to manage their finances. There is a legitimate concern that DHS’s scanning program will be viewed as a tool to harass racial and ethnic minorities. Businesses that use prepaid cards to pay wages and salaries should be prepared to answer employee questions about the DHS program and have a contingency plan in place should employees request to be paid with a more expensive and cumbersome check.

While the FinCEN reporting requirement would apply only to prepaid cards, border agents have no reliable way to distinguish prepaid cards from other types and it appears they plan simply to scan all cards they encounter in a traveler’s physical wallet or stored in a digital wallet on their mobile phone. Consequently, while the reporting requirement only applies to users of prepaid products, Homeland Security appears prepared to use the rule to obtain financial information about practically everyone who crosses the border.

DHS also intends to seize funds associated with prepaid cards it detects at the border. Presumably this power will primarily be used against prepaid cardholders who fail to make a correct disclosure under the FinCEN rule. As noted above, the distinctions between prepaid and debit cards are probably too nuanced for the general public to understand. Some people will not understand that the FinCEN reporting requirement applies to them and will fail to make a proper disclosure, thus subjecting themselves to seizure of their funds. While the possibility of this happening may seem remote, law enforcement has become increasingly aggressive with its seizure authority, the proceeds of which supplement strained agency budgets. More importantly, the people who are most likely to have their funds seized are among our most vulnerable people: senior citizens living on Social Security, workers out of a job receiving unemployment insurance, and single mothers for whom the state is collecting child support from non-custodial parents. Seizing the money that these people need to live on seems an overly severe punishment. Homeland Security should not have the authority to use asset forfeiture to enforce a confusing disclosure requirement.

The Program Violates the Right to Financial Privacy Act

Homeland Security’s plan to scan payment cards at the border in order to obtain financial information about travelers also raises obvious concerns about privacy. In particular, the program appears to violate the Right to Financial Privacy Act (RFPA) which prohibits financial institutions from providing federal agencies with the financial records of a customer except in certain limited situations. Under that law, release of financial records is generally only permitted with the customer’s consent or if the agency obtains a warrant, court order, or subpoena and, even then, only after the customer has been notified of the disclosure and has had an opportunity to object. When DHS scans a card at the border, it is sending a request for balance information about the card to the financial institution that issued the card. Such a request is prohibited under RFPA unless the agency has obtained consent or a warrant, court order, or subpoena – none of which will be happening. A financial institution that discloses records in violation of the RFPA is subject to significant civil penalties.

DHS takes the position that the RFPA does not apply to prepaid cards because they are not the same kind of account as a checking or savings account. Typically, when an issuer sets up a prepaid program, it opens an omnibus account which holds all of the funds for all of the cards in the program. The financial institution then creates sub-accounts within the omnibus account for each prepaid card it issues. This structure is used for ease of accounting and processing and the cardholder is generally unaware of and unaffected by it. DHS seems to think that this account versus sub-account distinction makes the RFPA inapplicable to prepaid. However, federal regulatory agencies that have looked at the question have concluded that despite their structural differences, there is no reason to treat prepaid cards and traditional bank products differently. For example, payroll cards, which are one type of prepaid card, are deemed to be accounts for purposes of Regulation E and the Electronic Funds Transfer Act. The Consumer Financial Protection Bureau has also proposed extending Regulation E to cover a broader range of prepaid products. Similarly, when the FDIC looked at whether deposit insurance was available to prepaid cards it concluded that the funds underlying these products “are no
different, in substance, than the funds underlying traditional access mechanisms.” Consequently, the FDIC extended coverage to prepaid cards that meet the general requirements for pass-through insurance. Financial regulators have not found the structural attributes unique to prepaid justifying treating the cards differently from traditional account products which suggests that prepaid should also not be treated differently for RFPA purposes.

More importantly, the U.S. Treasury’s Financial Management Service has concluded that the RFPA applies to Direct Express, its own prepaid product. Millions of Americans are currently using Direct Express to access their Social Security and other federal benefit payments. Treasury conducted a detailed analysis of the privacy issues that surround prepaid cards and, after consulting with regulatory agencies, consumer groups, Congress, and the general public, concluded that the RFPA does not cover prepaid products.

DHS’s position that RFPA does not protect prepaid is in direct conflict with the conclusions reached by the Treasury Department and is inconsistent with the views taken by federal financial regulators. Moreover, assuming RFPA does not apply to prepaid cards, it still applies to debit and credit cards and DHS’s plan is to scan all payment card types. Even if prepaid cards are not covered by RFPA, DHS would be acting contrary to the statute when it obtains financial records tied to other types of payment cards. No matter how you interpret the statute, Homeland Security’s program appears to have significant RFPA problems.

In addition to problems it may create for the government, DHS’s RFPA violations will create substantial liability for card issuers. Every time a bank responds to a balance inquiry or transaction from DHS, it will be subjecting itself to civil liability to cardholders. The law allows customers whose financial records are improperly disclosed to recovery actual and punitive damages along with statutory damages of $100. That means every DHS transaction subjects issuers to financial loss even if the customer has no direct harm. If DHS limits the scanning of payment cards to a small percentage of the 350 million travelers it inspect each year, the potential liability could still be enormous. Facing this level of risk, financial institutions may consider taking steps to insulate themselves from liability for DHS’s legal violations. One option would be to modify card processing systems to identify and reject the illegal transactions. If a number of issuers choose to block DHS transactions in self-defense, however, the government’s scanning program would certainly be a failure.

**Conclusion**

Homeland Security’s new program to stop individuals at the border in order to scan their payment cards, obtain information from their financial institutions, and potentially seize funds associated with the cards raises serious legal questions. It will invade the privacy of travelers and, in the process, violate federal law. Recipients of state and federal benefits along with other people who cannot afford a bank account will be called out at the border, subjected to additional scrutiny, and potentially turned into inadvertent law breakers. Financial institutions may incur significant liability because of the government’s illegal actions. Can these harms be justified for a program that is unlikely to identify or prevent significant amounts of money laundering? DHS should be required to address these legal and operational deficiencies before it moves forward with the program.

Stephen T. Middlebrook is general counsel at FSV Payment Systems, Inc., in Jacksonville, Florida. The opinions expressed in this article are those of the author, and may not necessarily be shared or endorsed by his employer.

**ADDITIONAL RESOURCES**

For other materials by this author, please refer to the following.

**ABA Web Store**

RFID, Near-Field Communications, and Mobile Payments: A Guide for Lawyers
From the Cyberspace Law Committee, Sarah Jane Hughes, Candace Jones, Stephen Middlebrook

Lawyers who advise companies using Radio Frequency Identification (RFID) devices or developing apps or managing data from RFIDs and other Near-Field Communications (NFCs) will need to keep pace with legal and regulatory developments from many quarters within and outside the United States.

Expert cyberspace law practitioners have ventured into uncharted legal and conceptual territory to advance the understanding of transactions in and affecting radio frequency identification, near-field communications, and mobile payments. The result is this cutting-edge book that will benefit lawyers and academics in explaining the basic issues, technology, and its application to others.
The United States National Security Agency (NSA) has recently been featured in news stories that detail, usually accompanied by a healthy dose of outrage, its data collection efforts. Sources claim that the NSA has been collecting hundreds of millions of records worldwide concerning private financial information, personal e-mail and contact lists, and other electronic data. “Big data,” as such data sets are often called, has an increasing presence in the world today. But the news stories raise more questions than they answer. Where does this information come from? Who collects this type of data? Who uses the information? To what ends? Are there laws that limit collection of use of this data? This article attempts to address some of these issues, with a focus on data relating to payment transactions.

What is Big Data?

“Big data” is a broad term that generally refers to the collection of large and complex data sets. Big data is often characterized by three defining characteristics: (1) the high volume of data collected, (2) the rapid velocity of collection and processing rates, and (3) the wide variety of data received and stored. Big data typically describes data sets that are so large that traditional data processing applications are not sufficient to manage and process the information. Instead, companies have developed, and continue to develop, new tools to handle and mine various aspects of the data sets. These tools enable companies to derive useful information from the massive amounts of data.

Big data comes from a variety of sources. The tracking of online shopping and banking give insight to customer preferences and payment information. In-store payment transactions also provide location information. Among other things, social media websites help gauge customer preferences and sentiment. Smartphone applications, online behavioral advertising and tracking, and geolocation services also serve as data sources. Rather than having an intended goal of gathering data, collection sources often create data sets simply as a byproduct of a company’s normal course of business.

New big data tools make it possible to aggregate this data from the various sources and to provide a more comprehensive picture of user sets. Often, data collected by a certain source at a specific point in time will have unforeseen uses in the future, especially if combined with data from other sources.

Although the term “big data” can describe a broad array of data collections, this article will primarily focus on a subset of big data – payments data. Payments data tracks purchases by individuals who use non-cash methods of payment, such as credit/debit/prepaid cards or online banking accounts. Payments data can provide information about individual consumers, such as what the individual is buying, how much he or she spends on certain items, where the person is located, and how much available money a particular consumer typically has to spend.

Who is Using It?

Payments data is being utilized by a variety of industries, including card networks, banking, retail, social media, service providers and data brokers, marketing, law enforcement, and intelligence.

The card industry uses payment data to a number of ends, including to cross-sell products, to create card-linked incentive programs, and to detect fraudulent use of credit cards.

Retailers are increasingly relying on big data. Daily deal sites, for example, use digital coupons to collect consumer information and then to analyze consumer supply and demand trends. The companies can track how issuing a promotion affects a business’s sales after the promotion has ended – including whether a promotion leads to increased repeat customers and/or a wider customer base. A certain luxury retailer developed both behavioral segmentation and a membership reward program based...
on information from big data. This has allowed the company to increase purchases of higher-margin products by its more affluent customers. One of the largest online retailers in the world stores information relating to searches, consumer recommendation, and merchandising. It uses information about a consumer’s purchases and “views” in order to recommend additional products. As another example, a major kitchenware retailer maintains customer databases with information about millions of households. The company tracks the income of a family, the value of its house, and the number of children in a family. This information allows the company to send targeted e-mails and increase the response rate. The company can also distribute different versions of its catalogs based on the preferences of different groups of customers.

As mentioned above, the public sector also collects and utilizes big data. In the United States, the NSA has been in the spotlight for its gathering of big data. News stories have reported that the NSA runs a project named “Follow the Money” that inputs financial data information in a system called “Tracfin.” Tracfin contains hundreds of millions of records collected about worldwide transactions, the great majority of which is comprised of credit card transactions.

**What is it Used For?**

Payments data is currently being used by many different industries toward many different goals, and undoubtedly more uses for this data will continue to emerge. Some applications of payments data include identifying consumers and their spending trends, constructing marketing campaigns, gauging the effectiveness of certain marketing efforts, setting product prices, determining which items to stock and in what quantities, making internal business decisions, preventing fraud, and building new aspects of a business.

**Identifying Consumers and Their Spending Trends**

Payments data is being used to help companies identify the characteristics of their customers, including their spending trends. This information can be focused on detecting specific patterns in the population at large, or certain large segments of consumers. Big data also enables customer micro-segmentation. Big data technologies allow companies to divide their consumer base into more and more granular segments, enabling marketers to track the behavior of individual customers and utilize this information. One large U.S. retailer has developed a program that can predict a woman is pregnant in the early stages of pregnancy (a so-called “pregnancy prediction score”). By tracking consumers’ purchases, and looking for slight changes over time (e.g., an increased purchase of lotion or certain supplements), the store is able to advertise to and draw in expectant mothers even before the more tell-tale baby purchases occur (e.g., diapers and formulas). One anecdote even tells that the company knew of a woman’s pregnancy before her father did, to his dismay.

Thus, payments data can provide a score of information about individual customers, varying from identifying social status to determining an individual’s “pregnancy prediction score.” Further, big data technologies allow companies to review this information almost instantaneously, providing the ability to adapt strategies almost in close to real-time.

**Constructing Marketing Campaigns**

A variety of industries utilize information derived from payments data in order to build marketing campaigns. For example, card transaction data allows banks to more accurately cross-sell its products to specific customers. Credit card companies also use payments data to create card-linked offers. These offers give cardholders savings in return for making specific purchases with a credit card. The payment data lets card companies better tailor the offers to specific customers.

Companies also utilize payments data in order to create loyalty and rewards programs. With this information, the companies can better identify customers’ wants and needs, and build programs that incentivize the consumers to spend with their company in order to earn credit toward desired products or services.

One marketing technology company reportedly will begin to roll out a new product that allows marketers to connect a person’s “digital persona,” despite discrepancies in the name used at various times or locations (whether due to a name change, use of a nickname, etc.). This will enable marketers to pull information from different databases (i.e., online sales databases and social media databases) for a more complete picture of the target consumer.

**Assessing the Effectiveness of Marketing Efforts**

Using payments data, a company can gauge the effectiveness of specific advertising efforts or incentive offers. Payments data enables companies to track customer purchases back to the originating source, whether it be Google, Yelp, or any of the countless other online advertising sources. This is known as “closing the loop” and allows merchandisers to identify, and perhaps increase the emphasis on, the most profitable sources of marketing.

**Price and Assortment Optimization**

Payments data enables a company to optimize its merchandise pricing; including decreasing the time it takes to make pricing decisions. Based on the granular data available on sales, retailers can employ the information available to assess past pricing decisions and to adjust future pricing. Retailers can also use big data to determine the inventory for specific stores based on information about local consumer demographics. Moreover, retailers can receive this information and make adjustments to price and inventory assortment almost instantly.

**Making Internal Business Decisions**

The use of payments data also allows companies to pursue a number of business objectives. A company can better predict trends and detect cost-savings sources. Analysis of such data can lead to greater efficiency and speed in a company’s business, as well as provide for improved moni-
toring of inventory for safety and quality.

**Prevention and Detection of Fraud**

Payments data may also help financial institutions and card companies to detect and prevent fraudulent card use. By identifying costumer characteristics and spending patterns, a company may be able to determine when certain transactions deviate from established patterns. A company could then investigate the questionable transactions further, and potentially prevent fraud before more damage has been done.

**Generate New Business**

A company may be able to generate a new business model for itself in the course of its collection of data. For example, a payments provider might create a new business by selling consumer insights based on the data it already generates while processing payments. There is talk of one digital coupon company doing just this. With an influx of competitors, it is possible that the company has maxed out its profits from the deals business, but along the way has gathered an expanse of data. The company has considered shifting its business model to increase the focus on providing consumer information to merchants and marketers.

**What are the Relevant Laws?**

The regulatory obligations regarding big data have been in effect for almost a decade. They include regulations concerning privacy and security, notice and consent, the collection of data and the targeting of that collection, access, and participation. The regulations come from both federal and state law.

The Federal Trade Commission (FTC) is the primary enforcement agency in the United States for privacy and data security issues. The FTC’s “enforcement authority in these areas arises under Section 5 of the FTC Act, which prohibits unfair or deceptive trade practices. Pursuant to this authority, the FTC has imposed data security obligations on all industries. The FTC also monitors data breaches and can file suit against a company for a broad range of allegedly unfair or deceptive practices, including privacy policies. The FTC established a division of Privacy and Identity Protection and issued its “Final Privacy Report” in March 2012, which includes guidelines and best practices for business and recommends a baseline federal legislative approach, but which does not contain legal requirements.

The FTC and several other federal agencies issued a joint Final Rule that imposes additional regulatory requirements on businesses, including employers, that provide consumer information to consumer reporting agencies. The Final Rule both requires businesses to ensure the accuracy of such information, and provides for challenges and dispute resolution.

The FTC enforces privacy policies and initiates enforcement actions against companies that do not abide by privacy and data security promises, or simply fail to implement “reasonable data security measures.” An FTC enforcement action may result in a settlement order that includes: statutory penalties to settle allegations of violations and requirements that the company establish, implement, and maintain a comprehensive information security program; obtain, every two years for the next 20 years, an audit from an independent third-party professional to ensure that its security program meets the standards of the order; remain subject to standard record-keeping and reporting provisions to allow the FTC to monitor compliance; and avoid future misrepresentations of the company’s security practices.

The Gramm-Leach-Bliley Act (GLBA) is a federal law that requires companies that offer consumers financial products or services such as bank accounts, loans, investment advice, or insurance, to notify consumers of their information-collecting and sharing practices. The GLBA also requires that they explain how the information they collect is used, as well as how it is protected. Several federal regulating agencies, including the FTC, have issued a model privacy notice form.

The Fair Credit Reporting Act (FCPA), also a federal law, regulates the collection, disclosure, and use of information that businesses use to make important decisions about consumers. Such information includes that pertaining to credit, insurance, check writing, insurance, medical records, and tenant history. The FCPA is enforced by the FTC and private parties.

The Payment Card Industry Data Security Standard (PCI DSS), which is a data security standard set by the payment card networks, has also been explicitly incorporated into law in some jurisdictions. For example, Nevada law requires Nevada businesses to comply with the PCI DSS in any transaction where the business accepts a credit card (or other payment card) for the sale of goods or services. The same law also requires Nevada businesses to encrypt any personal information the business transfers outside of its secured systems (e.g., PDA, thumb drive, lap top, e-mail, etc.).

Regulation of big data at the state level stems from multiple sources. Some state regulation is actually enforcement of federal law. For example, the state attorneys general have authority to enforce several federal statutes. States have also enacted their own laws regulating big data. These laws include unfair and deceptive trade practices acts (sometimes referred to as “baby FTC acts”), as well as state privacy and data security acts. State laws generally prohibit requiring an individual to transmit his or her social security number (SSN) over the Internet unless the connection is secure or the number is encrypted. Similarly, they also generally prohibit requiring the use of a SSN to access a website unless a password or other unique personal identification number is also required.

California has long been on the forefront of privacy and data protection development, often serving as a bellwether on these issues. The recent Do-Not-Track Bill is one of the state’s latest steps to strengthen consumer privacy protection. Amending the California Online Privacy Protection Act (CalOPPA), the Do-Not-Track Bill (A.B. 370) was unanimously passed by the California Senate and Assembly in late August of this year. The bill adds new disclosure requirements for operators of commercial websites and online services concerning...
(1) how they respond to “do not track” mechanisms exercised by consumers, and
(2) whether third parties may collect personally identifiable information on their websites when a consumer uses such a website.

Prior to the August amendments, CalOPPA generally required the conspicuous posting of a privacy policy that describes (1) the categories of personally identifiable information that the operator collects about individual consumers who use or visit its website or online service, (2) third parties with whom the operator shares the information, (3) the process by which consumers can review and change the collected personally identifiable information, and (4) the process by which the operator will notify consumers of changes to its website’s privacy policy. A party violates the statute only if it fails to post its privacy policy within 30 days after being notified of noncompliance. These requirements remain in place even after the amendments.

In order to heighten consumer awareness of online behavioral tracking, the Do-Not-Track Bill adds the following two disclosure requirements to CalOPPA for operators of commercial websites and online services that collect personal information from consumers who visit their sites:

1. Disclose how the operator responds “to ‘do not track’ signals or other mechanisms that provide consumers a choice regarding the collection of personally identifiable information about an individual consumer’s online activities over time and across different Web sites or online services;” and
2. “Disclose whether other parties may collect personally identifiable information about an individual consumer’s online activities when a consumer uses the operator’s Web site or service.”

Despite its popular name, the CalOPPA amendments do not actually impose a “do not track” (DNT) standard on websites. The bill merely calls for the disclosure of how a website or online service operator will respond to a consumer’s DNT request.

The Do-Not-Track Bill permits an operator to satisfy this disclosure requirement by posting a hyperlink “to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer [the ability to make a DNT request].”

It is clear that big data, and especially consumer payment data, is a valuable commodity. As more uses for consumer payment and behavior data are developed, we can look forward to more laws to regulate how such data is collected and used.

Veronica K. McGregor is of counsel at Jones Day in San Francisco. Sophia Helena Calderón and Roberta D. Tonelli are associates at the same office.
The Past and Future of Bitcoins in Worldwide Commerce

By Denis T. Rice

Virtual currency is not new. It has been around since the early 2000s in virtual world websites like Second Life and online role-playing game sites like World of Warcraft, where virtual currency is “earned” by completing virtual quests. But neither Linden Dollars earned in Second Life nor Facebook credits earned on Farmville could be spent outside of their restricted virtual worlds, even though some could be exchanged for dollars (or other real world currencies) on third-party websites. The bitcoin is changing this landscape. Some hail it as “the next great step in Internet and global currency.” (Although “bitcoin” is capitalized by some writers; the author elects to treat the word generically and use the lower case throughout.)

Bitcoin started in 2008 with a self-published white paper by a group of computer geeks using the fictitious name “Satoshi Nakamoto.” A bitcoin is essentially just a snippet of code, based on an algorithm first identified in the Nakamoto white paper. In 2009, the Bitcoin Network was established and actual bitcoins were first issued and its evolution since has been swift. Practitioners in cyberspace or commercial finance law need at least a working knowledge of this digital currency which has no borders and is unregulated by any governmental authority or central bank.

A central purpose of bitcoin according to Nakamoto was to reduce transaction costs incurred when parties validate transactions and mediate disputes. To that end, the bitcoin system is based on open source computing. Bitcoin users cooperate to validate transactions either by running a program implementing the bitcoin protocol on an individual’s own computer or by creating an account on a bitcoin website to run the protocol. Although creators of bitcoins originally used them for Internet-related tasks, like trading bitcoin for programming help, the currency has gained increasing acceptance in broader contexts.

The early use of bitcoin in online drug markets and casinos gave it a somewhat tarnished reputation. But bitcoin increasingly is used in legitimate commerce. Thus, early this year, Coinbase, a bitcoin payment processor, reported selling $1 million in bitcoins in one month at more than $22 each. Later, venture capitalists began pouring millions into startups that focus on bitcoins. In July 2013, the Winklevoss twins (of Facebook fame), having formed an electronically traded fund called the “Winklevoss Bitcoin Trust,” filed with the U.S. Securities and Exchange Commission (SEC) to sell shares in the trust to the public.

Creating Bitcoins

Bitcoins are created by “mining.” Bitcoin miners engage in a set of prescribed complex mathematical calculations in order to add “blocks” to the “block chain,” which is a transactional database shared by all nodes participating in the bitcoin system. The full block chain contains every transaction ever executed in bitcoin, starting with the very first one which is called the “genesis block.” This allows determination of the value belonging to each address at any point in time. Miners who succeed in adding a block to the block chain automatically receive a fixed number of bitcoins as a reward for their effort.

Space does not permit a detailed description of the mining process, but in essence a miner maps an input data set (i.e., the block chain plus a block of the most recent Bitcoin Network transactions and an arbitrary number called a “nonce”) to a desired output data set of predetermined length (the “hash value”), using Nakamoto’s algorithm. The miner then “solves” a new block by repeating this computation with a different nonce until hash of a block’s header having a value not more than the current target set by the Bitcoin Network is generated. Because each unique block can only be solved and added to the block chain from one source, all individual miners and mining pools in the Bitcoin Network are competing. Such competition spurs them to constantly increase their computing power in order to improve their ability to solve for new blocks. A miner can only build onto a block (referencing it in blocks the miner creates) if it is the latest block in the longest “valid” chain. A chain is valid if (1) it starts with the genesis block and (2) all of
difficulty in finding valid hash values has to mining increases (in order to maintain a computer processing power dedicated to power the hardware).

For producing bitcoins, with the deal also of high-end servers designed specifically for mining, and the newest rigs use an application-specific integrated circuit (ASIC) built for increasing, and the newest rigs use an application-specific integrated circuit (ASIC) built for excessive production unless the Bitcoin Network’s source code and the underlying protocol for bitcoin issuance are changed.

The targets established by the Bitcoin Network constantly increase in difficulty, meaning that miners constantly need more expensive processing power to compete. Early on, a bitcoin could be bought for 25 cents on an exchange, and a miner with just a laptop’s CPU could make a handful of new bitcoins a day. Computers now are specially designed solely for bitcoin mining, and the newest rigs use an application-specific integrated circuit (ASIC) built specifically to execute the hash operation. This bitcoin “arms race” led to a 2013 venture funding of $200 million in the maker of high-end servers designed specifically for producing bitcoins, with the deal also including the maker of state-of-the-art microchips to power the hardware.

The current mining protocol makes it increasingly difficult to solve for new blocks as computer processing power dedicated to mining increases (in order to maintain a 10-minute per block average). Because the difficulty in finding valid hash values has grown exponentially since the first block was mined, one individual can no longer mine bitcoins successfully. Mining “pools” have formed, in which multiple miners combine their processing power. When pool members solve a new block, they allocate the reward according to the processing power each contributed to the solution. Such pools give participants access to smaller, but steadier and more frequent, bitcoin payouts. The Wall Street Journal reported on November 6, 2013, that the speed of bitcoin mining was now 40 times faster than in January 2013. It was estimated in August 2013 that about 11.5 million bitcoins were in existence, with the amount steadily increasing. Estimates are that 90 percent of the 21 million bitcoin limit will have been produced by 2020.

The Bitcoin Network is designed so as to decrease the reward for adding new blocks to the block chain over time. Ultimately, miners will need to be compensated in transaction fees in order to provide adequate incentives for miners. (However, as of publication of this article, transaction fees still accounted for but 1 percent of miners’ total revenues.)

Trading For Bitcoins

To buy or sell bitcoins, one must have Internet access to the Bitcoin Network, where such transactions are consummated within seconds. Double-spending of any single bitcoin is avoided by having the user give information on the transaction to the Bitcoin Network of the transaction, which uses the block chain to memorialize every bitcoin transaction.

A bitcoin trader first installs on a computer (or mobile device) a software program allowing the trader to generate a digital “wallet” for storing bitcoins. The wallet can either be stored in the trader’s own computer or hosted on a third-party website. The trader then connects to the Bitcoin Network and engages in the purchase, sale, and receipt of bitcoins. A trader can have an unlimited number of digital wallets, each with a unique address and verification system consisting of both a “public key” and a “private key.” Because the system relies upon peer-to-peer networking and cryptography, it is a distributed model resistant to central control. The private key, used to authorize bitcoin transactions, has no information about the user, although the transactions are traceable by means of the public key. The result is that the address of a bitcoin is traceable on an individual’s own computer, but ownership of each address remains anonymous.

One way to buy bitcoins is to identify someone willing to sell bitcoins, then offer to buy them with conventional currency. Once a price is set, the seller transfers the bitcoins to the buyer’s wallet. Another and more organized way is to use a bitcoin exchange. As with conventional currency exchanges, price is usually not individually negotiated, but instead based on the aggregate supply of and demand for bitcoins in the system. While using an exchange adds to the transaction cost, it is both more efficient and better monitored.

There are estimated to be approximately 12 currency exchanges around the world where consumers and businesses can trade bitcoins for local currency. Because the technology is open source, new services are created almost every week. Among the more active are Mt. Gox in Japan, BitBox and Bitstamp in the United States, and Bitcurex in Poland. Banks like Morgan Stanley and Goldman Sachs reportedly visit bitcoin exchanges up to 30 times a day. Bitcoin exchanges are not problem-free: Mt. Gox in Tokyo, the largest exchange, reported in 2013 that its services had been disabled for hours by an Internet “denial-of-service” attack. Mt. Gox said attackers wait until the price of bitcoins reaches a certain value, then sell, destabilize the exchange, wait for panic-selling to cause the bitcoin price to drop to a certain amount, then stop the attack and start buying as much as they can. Such volatility caused bitcoin to rise from roughly $5 in June 2012 to a high of $266 in April 2013, before dropping to $108 in May 2013.

Using Bitcoin in Day-to-Day Commerce

A retail customer can pay in bitcoin by using a smartphone to scan a barcode provided by the retailer. Retailers see an advantage in avoiding credit card fees that
can run as high as 3 percent, compared to less than 1 percent for bitcoins. Moreover, bitcoin transactions are final, whereas credit card charges can be disputed. This kind of advantage helped BitPay, Inc., of Atlanta in 2012 sign up more than 8,000 merchants worldwide to accept bitcoins and to set what was then a new record for bitcoin payment processing, with orders and payments from 17 different countries such as Belgium, Russia, and Poland. Since bitcoin is a currency run by those who use it, a bitcoin’s value is determined by the marketplace; in other words, a bitcoin is worth whatever someone will take for it.

Venture Capital and Bitcoin

Startups focused on marketing bitcoin services have attracted increasing interest from venture capitalists. For example, in 2013, venture firms invested more than $2 million in OpenCoin, Inc., and $5 million in Coinbase, which operates an online service allowing users to buy and store bitcoin in a digital wallet and pay merchants for goods and services. Coinbase claimed some 116,000 members who had converted $15 million of real money into bitcoin, and dollar conversions increasing by about 15 percent a week. The San Francisco venture firm Kleiner Perkins Caufield & Byers reports that it is exploring bitcoin-related investments and has reviewed over two dozen companies.

Electronically-Traded Funds

As noted earlier, the Winklevoss twins filed a registration statement with the SEC in 2013 for their “Winklevoss Bitcoin Trust,” an ETF. The filing, which contains over 17 pages of “Risk Factors,” observes that (1) the value of bitcoins is determined by the supply of and demand for bitcoins in the bitcoin exchange market, as well as the number of merchants that accept them, and (2) bitcoins have little use in real-world retail and commercial markets compared with their “relatively large use by speculators.” Columnist Chuck Jaffe opined that the twins face a long, uphill battle just to get their fund to market, adding that “chances are good it will still be viewed for years as a granular, niche fund – more like one specializing in Bulgarian stocks than with mainstream applications.”

Regulatory Issues

Bitcoin faces a number of unresolved regulatory issues. They involve FinCEN, the U.S. Department of Justice, the SEC, and state regulators of money service businesses (MSBs). As mentioned earlier, FinCEN this year issued regulatory guidance classifying digital payment systems like bitcoin as “virtual currencies,” on the basis they are not legal tender under any sovereign jurisdiction. While opining that a user of virtual currency is not an MSB and hence not subject to federal MSB regulation, FinCEN went on to state that U.S. entities that generate “virtual currency” (including bitcoins) could be deemed MSBs if the virtual currency were sold for “real currency or its equivalent.” Thus, miners of bitcoin within the United States may need to register and comply with federal MSB regulations if they sell bitcoins for dollars. American Banker online has asserted that at least three U.S. bitcoin exchanges elected to shut down as a result of FinCEN’s guidance. FinCEN’s director stated that its guidance aims to protect digital currency systems from abuse and ensure that information is available to prosecute “criminal actions,” and is not aimed at everyday bitcoin users.

In May 2013, the Department of Homeland Security seized an account controlled by Mt. Gox on the theory that the Japanese exchange was operating as an unlicensed MSB. Mt. Gox subsequently registered with the U.S. Treasury as an MSB. The various regulatory issues surrounding bitcoin has prompted bitcoin enterprises to form a self-regulatory group called the “Committee for the Establishment of the Digital Asset Transfer Authority,” which intends to set technical standards aimed at preventing money-laundering and ensuring compliance with laws.

Fifty states also have laws regulating MSBs. Several, including California and New York, have reportedly warned companies involved in bitcoin that they may be violating such laws. Indeed, the California Department of Financial Institution already has in its files a detailed letter from a law firm on behalf of the Bitcoin Foundation, arguing that California’s law, the Money Transmission Act, has no application to bitcoins.

Turning to securities laws, in July 2013, the SEC filed a civil action in federal court in Texas, charging an individual and his company with using a bitcoin-based Ponzi scheme to defraud investors. The SEC alleged that the founder and operator of Bitcoin Savings and Trust had offered and sold bitcoin-denominated investments through the Internet using the monikers “Pirate” and “pirateat40.” The company allegedly received $700,000 bitcoins from investors valued at more than $4.5 million, based on the average price of bitcoin when the investments were sold.

The SEC claims the company was a “sham” where bitcoins from new investors were used to pay interest of up to 7 percent per week to existing investors and also to cover investor withdrawals. The SEC further alleges that the founder diverted investors’ bitcoins to trade for his own account on a bitcoin exchange and to trade for dollars in order to pay personal expenses. Such acts are alleged to violate the anti-fraud and registration provisions of Sections 5(a), 5(c), and 17(a) of the Securities Act of 1933, Section 10(b) of the Securities Exchange Act of 1934, and SEC Rule 10b 5.

Criminal Issues

Two federal criminal indictments in 2013 have somewhat tarnished the bitcoin image. An indictment of Liberty Reserve, S.A., a Costa Rican currency exchange, and seven of its executives by a grand jury, alleged that operators of the exchange used bitcoin to run a $6 billion money-laundering operation in violation of Section 311 of the USA PATRIOT Act and provided a central hub for criminals trafficking in everything from stolen identities to child pornography. Prosecutors asserted that Liberty Reserve’s trading in bitcoin provided the kind of anonymous and accessible banking infrastructure increasingly sought by crimi-
nal networks, which they said “heralds the arrival of the cyber age of money laundering.”

Finally, October 2013 saw the federal government indict and shut down the “Silk Road,” an online marketplace where millions of bitcoins allegedly were swapped for drugs and black market products. As news of the shutdown spread, bitcoin values tumbled, initially dropping by about 20 percent (or close to $500 million) before turning around. On the Bitstamp exchange, bitcoins dropped from about $125 to $90 before climbing back to $115. Values on the Mt. Gox exchange dropped from $140 to $109 before returning to $128. The government simultaneously arrested Ross William Ulbricht, who allegedly operated the Silk Road website using the alias “Dread Pirate Roberts,” and who now faces drug trafficking, money laundering, and hacking charges. The FBI filed an affidavit in the case which asserts that digital currency is not just used in the black market, but can serve criminal purposes because of the ease of moving money anonymously.

The Future . . .?

The economist Paul Krugman stated earlier this year that, unlike gold or paper fiat currencies, bitcoin derives its value solely from a self-fulfilling expectation that others will accept it as payment. Herb Jaffe cited a Morningstar analyst as having called the Winklevoss ETF “a total gimmick,” that bitcoins are very illiquid, and that the current trading infrastructure “is riddled with security/efficiency problems.” Others see bitcoin as a major development in virtual currency. Robin Harris on ZDNet asserts that bitcoin or something like it is not going away, observing that dollar/gold convertibility ended in 1971 and floating exchange rates have prevailed since. There are many areas where the future of bitcoin is yet to be developed: Is it an investment? How will transactions be taxed? What will be the effect of China’s recent entry into the bitcoin market? In 2014, we can expect some answers, but also many new questions.

Denis T. Rice is senior counsel at Arnold & Porter LLP in San Francisco. The author offers his thanks to partner Robert L. Taylor of Arnold & Porter for a review of patents possibly bearing on bitcoin.
On August 12, 2013, University of Washington computer science professor Rajesh Rao sat in his lab playing a video game. Rao could see the video game, but he didn’t hold a game controller. Instead, across campus at the same time, fellow researcher Andrea Stocco had his hand on the game controller, but Stocco couldn’t see the game.

Rao, wearing a cap filled with electrodes to read his brain signals, simply thought about specific movements of the game controller, while Stocco, wearing a cap with a transcranial magnetic stimulation coil placed directly over his left motor cortex, involuntarily moved his right index finger to push the game controller, firing a cannon in the video game. Without invading either head, the two researchers were able to share directed thoughts, over a distance connected by the Internet. Rao’s cap captured his “brainspray” – brain signals available for capture and interpretation outside his head – and sent the precise signal to Stocco, whose brain accepted the signal and instructed his body to act on it. “The next step,” said Rao, “is having a more equitable two-way conversation directly between the two brains.”

As demonstrated below, humanity has entered into an era where the deep study of our brains is combining with sophisticated technology to project brain signals, to interpret brain signals, and to transform brain signals into physical action. Once the realm of science fiction, businesses currently exist to allow brainspray control of mechanical objects. For years, scientists have been able to see into our brains, capturing and measuring response to stimuli, but now they can accurately interpret what those signals mean and relay them into actions that can fly a drone or help a person who has lost use of his or her arms to feed him or herself. In addition, technology tends to become cheaper and easier to use over time, so we should expect dynamic growth in the field of capturing and applying brain signals. This technology can provide benefits beyond imagination to the injured and infirm, can make our soldiers and pilots more efficient, and can lead to consumer and business product interfaces controlled through directed thoughts alone.

While we are well on our way toward realizing these benefits to society, we are not adequately prepared as a society for the regulation of this technology. Clearly we have no current laws distinguishing between the legitimate and illegitimate use of technology to capture someone’s brain signals without that person’s consent, not to mention the technology that can force bodily action through brain stimulation alone. We have no rules about storing and using the brain signals of another person and the intellectual property that might arise from these signals. In the United States, our legal protections for personal privacy are riddled with gaps encompassing the current technology, and larger gaps for the invasive technology that will arise in this area. In short, we are ill-prepared for the brainspray revolution, and we should be examining policy options before it is upon us.

Brainspray: The Current Applications and Research

Brain signal capture and application is not a speculative future advance, but a set of technologies that exists right now. Businesses are using directed thoughts to create consumer toys that play games and move objects in the real world. Doctors are capturing brainspray to help enable people who have lost the use of important body parts and functions. Researchers are peering into brains and interpreting or applying the information they find there. New technologies are developed or expanded to capitalize on each of these advances, but the technology and knowledge we currently possess is already impressive.

In November of 2012, a California company called Puzzlebox published a plan on the business crowdfunding site Kickstarter. Puzzlebox was raising money by promising to deliver a small remote-controlled helicopter globe that used an electroencephalogram headset, plus a mobile phone to fly the drone helicopter only by the user’s thoughts. Unsurprisingly, Puzzlebox quickly completed funding through Kickstarter to build and sell the MindWave Mobile compatible brainwave controlled
helicopter. Puzzlebox’s partner in this venture, NeuroSky also sells a set of “cat ears” that a person can wear, which express the wearer’s mood by capturing brain signals and turning them into movements of the furry appendages. In a less frivolous application of the technology, NeuroSky sells the MindWave headset to monitor attention levels of students as they react with mathematical, memory, and pattern recognition applications. The company also sells its brainwave sensing technology chips to other companies who wish to create completely new applications.

Another company offering an electroencephalographic reading helmet is Emotiv Lifescience, whose CEO Tan Le is a well-known evangelist for controlling machines through a brain interface. Emotiv’s brainwave readers are being used by the Grateful Dead’s Mickey Hart to make music simply by thinking of the sounds, and by a Chilean company to create three-dimensional objects by picking shapes from a screen with directed brain waves. Emotiv equipment has been used to operate video games, and German engineers in Berlin have built an Emotiv brain interface into a car’s controls, although they have not produced a roadworthy product yet.

Emotiv brain helmets have helped create the world’s first thought-controlled wheelchair in Japan, and scientists in Switzerland have built on the concept to allow “shared control” between the brain and the sensors in the chair itself. The shared control is easier for the chair’s controller, who does not need to give every command to make the chair move or stop.

Clearly an important task for brain-controlled devices is assisting people who have lost limbs or abilities. For example, Ambient Corporation has developed a neckband that reads thought directions for about 150 words, and then wirelessly signals those words to a computer to voice the thoughts out loud. There are clear applications for this technology in silent voice commands for military operations, and the U.S. Army has already invested in transcranial ultrasonic stimulation helmets to transfer orders and affect soldier’s brains. CBS news magazine, 60 Minutes, and ABC News featured University of Pittsburgh researcher Andrew Schwartz, who has been working since 2006 to find ways for a person to control a robotic arm with only brain signals. Working with Dr. Schwartz, surgeons implanted four microchips in a paralyzed patient’s brain that translate her brain’s signals into movement of a robotic arm. As demonstrated on television, the patient can feed herself through thought instructions alone.

Other instances of “bionic” limbs controlled by directed thoughts include former Army Staff Sergeant Glen Lehman, wounded in Iraq, who can manipulate a prosthetic arm with his mind, including drinking coffee and bouncing a tennis ball. The Defense Advanced Research Projects Agency (DARPA) is funding research in prosthetics controlled by mind signals to address the problems raised by the more than 2,000 U.S. service members that have undergone amputations since the year 2000. The DARPA projects not only focus on signals from brain to arm, but have made strides in the important field of reverse signals from the prosthetic arm back to the brain of a subject. One DARPA funded prosthetic connects the nerves of an amputated limb to enable a sense of touch with neural feedback similar to a natural arm.

An entirely different technology is also spawning applications to read a subject’s brainspray and turn those thoughts into physical action. The Functional Magnetic Resonance Imaging (fMRI) machine measures blood oxygenation and flow in the brain and is known for such diverse tasks as brain mapping for clinical use and discovering a “sixth sense” of numerosity in the human brain. The technology allows researchers to identify which areas of the brain activate when certain emotions are evoked, and fMRI has been used commercially for lie detection and advertising evaluations. Honda has applied fMRI brain reading technology to create a helmet that allows its wearer to move a humanoid robot by simply thinking about what appendage to operate. By imaging the movement of his or her right hand, the helmet-wearer can operate the right hand of the robot.

These varied technologies and applications are only a launching pad from which humanity will grow an entire body of science and tech built around a brain-machine interface, allowing people to control an entire range of physical movements and tools – from cars to robots to war machines – with directed thoughts. This science also allows intrusive capture of brainspray, and the tools to interpret the captured signals.

In some cases, we have already seen how machines can stimulate a body’s involuntary movement by triggering reactions in the brain. And like all useful technology, enormous sums of money will be spent by governments, businesses, and health researchers to make these tools more effective, less expensive, and easier to use.

Legal Issues and Regulation of Brainspray

As this technology develops, legal and ethical questions will increase. Who owns the information generated by a person’s brain that is captured by technology created and refined by a company or government? When does the interpretation of brainspray trigger privacy laws? How far can anyone go in reading the thoughts of a person without that person’s permission? What kinds of laws can be affected by brain-to-machine interfaces?

The privacy implications of a brain-machine interface are similar to those that exist now on the Internet. Just as a deep knowledge of a person’s Internet surfing and searching can provide a distinct picture of that person’s thoughts and priorities, the ability to capture someone’s brain signals and interpret them would tell an intimate story about that person. Similar to current personal Internet records, we would be concerned about our interior thoughts being exposed to business and government, as well as to predators and even certain neighbors or family members. Any of these people or organizations could use our Internet records or our direct thoughts against us in many uncomfortable ways. And of course, in the United States, we have very little effective regulation about who can see our Internet activities, and the recent National Security Agency scandals have shown us
that even where laws exist to protect our privacy, institutions and individuals are finding ways around them. This is likely to be equally true when the information sought is the direct brain connection of an individual, just as it is true for that person’s Internet activity. Without more effective laws protecting personal privacy, it is likely that Americans will be vulnerable to an onslaught of thought capture as the technology improves to harness brain signals.

It seems the most obvious legal problem with the ability to capture and interpret brainspray is the possibility that someone will use the technology to invade another person’s thoughts without that person’s consent. And like many places in the law where a person’s consent is required, the method of attaining and then proving consent may be difficult to prove. In many cases, consent may simply be a matter of acquiring a confirmation signature prior to using a person’s private financial or health care information. But many messy aspects of life make proof of consent a dicey topic. For example, after taking pictures at a crowded festival, a photographer is likely to find it impossible to track down specific photographed individuals if he she decides to use the pictures commercially. The medical establishment has not always requested consent for use of tissue samples in research, and often the tissue donors have passed away before the question arises. Two decade’s worth of police procedural have been based on the difficulty of proving consent, or lack of consent, in sexual relations. If the technology advances enough for law enforcement, government, or even an employer to read a person’s brainwaves without that person’s knowledge, when would consent be needed and what kind of consent would suffice?

The law frequently acknowledges that context is important in regulating behavior. It might make a difference why the brainspray is being accessed in the first place. By analogy, not every release of a person’s medical or health information is protected by the medical privacy laws in the United States. A patient who allows collection of DNA for medical treatment is protected under the privacy sections of HIPAA, but a suspect who allows collection of DNA by the police for an identity match may not have that DNA protected as private under the law, and a person who sends his or her DNA to a private lab for a heritage review analysis is not protected under the law, only the lab’s voluntary privacy policy. Similarly, under the U.S. business-friendly privacy laws, if a retailer reads the brainspray of customers at the checkout line to check for shoplifting or to analyze each customer’s satisfaction at the shopping experience, nothing under current law would be likely to prohibit those actions; especially if the retailer offered a discount on sales to customers who allowed such a passive examination (“VIP card customers get 10 percent off on ice cream in exchange for passive satisfaction reading of brain waves”). Currently, Google is able to look inside all e-mails that pass through its servers and to keep records of all of the searches you perform with its tools, so how much more intrusive is a painless passive quality check of brainspray in passing? If courts and legislatures are not prohibiting these activities, they may remain afloat about limiting further data collection from consumer’s brains.

However, it does seem likely that private commercial use of brain signal capture technology will raise the concern of judges, if not legislatures. While new laws may be passed to address this issue, older rules may be stretched to fit this situation as well. We can see this trend in a ruling filed the week this article was written, where a three-judge panel of the Ninth Circuit Court of Appeals upheld a lower court’s ruling against Google for invasive intrusion into people’s private space. Joffe v. Google, D.C. No. 5:10-md-02184-JW (9th Cir., Sep.10, 2013). Google contended that its apparently random “war driving” capture of private information from unprotected Wi-Fi in people’s homes and businesses could not, by law, be considered wire-tapping under the definition of the federal and state wire-tapping statutes, because unencrypted Wi-Fi data could be picked up by anyone with the right equipment. The court clearly felt that using sophisticated listening systems to capture information that people considered private may well cross some kind of legal line, and wire-tapping was the closest line available. Judge Bybee wrote, “Even if it is commonplace for members of the general public to connect to a neighbor’s unencrypted Wi-Fi network, members of the public do not typically mistakenly intercept, store, and decode data transmitted by other devices on the network.” When Google argued that anyone who purchased a certain spy device could read unencrypted Wi-Fi signals, the court refuted this argument by stating, “A device that surreptitiously logs a computer user’s keystrokes can be purchased online and easily installed, but that hardly means that every keystroke – whether over a wired or a wireless connection – is “readily accessible to the general public.” Similarly, using sophisticated equipment to capture the most intimate and personal of signals for private gain may be too much for a court to tolerate, and it may co-opt an existing set of laws as basis for prohibiting this behavior.

Similarly, if the technology for brain signal capturing became pervasive and inexpensive, how would we regulate a prospective father-in-law testing the intentions of his daughter’s suitor? Would we find it problematic that a new generation of spouses would be able to tell if their mates were being honest about that late night of working, or even about whether the spouse really looks fat in those new pants? And when teenagers gain access to the brainspray readers, could we expect mature and sober evaluations of friends, love interests, and parents? Would there be age restrictions on appropriation and application of brain signal analysis? Are these everyday applications too insignificant to become a source of regulation, or is the invasion into a person’s thoughts simply too creepy to be allowed at the most personal levels without consent? And then again, how would we measure coercion of that consent? The most quotidian tasks and interactions of our lives will be altered forever when others can know our thoughts and emotions with more precision. Etiquette would likely
instruct us that unauthorized brain reading is rude and inappropriate, but many of our civilized customs are not enforceable in law. As many an attorney has told a pleading client with a tenuous claim, there is no law against being a jerk, so passive personal al use of brain signal technology may be tolerated by the law, even if frowned upon socially.

If an employer captured and analyzed brain signals for job purposes, then state employment laws and federal labor laws are likely to provide some limitations, just as the U.S. National Labor Relations Board has been recently aggressive at limiting employer’s use of social media complaints in union organizing campaigns, and just as several states have restricted employers from forcing employees to provide passwords to private accounts. See The NLRB and Social Media, www.nlrb.gov/node/5078; and Employer Access to Social Media Usernames and Passwords, www.nels.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx.

The asymmetrical power relationship between employer and employee often triggers concerns about fairness that may not exist in other situations. The existence of a separate set of employment regulations would also make it easier to limit intrusive brain studies in employment as part of the nation’s industrial policy. The same may be true for education, where many parents would be concerned about the school administration examining a student’s moods and thoughts, rather than evaluating him or her on classroom behavior.

Under U.S. laws, access of private data by law enforcement is a special case and may raise Constitutional concerns. The Fourth Amendment promises us security in our persons, houses, papers, and effects against unreasonable searches and seizures. Because the technology is in its infancy, it seems unreasonable that police would investigate or interview us in a manner that allows our own thoughts to be read from outside our head. We would not know how to guard against such intrusion. When the government even passively reads a citizen’s brainspray, the government is likely violating the Fifth Amendment as well, forcing a suspect to incriminate him or herself as his or her brain provides the vital information needed to arrest and convict. But once we become used to passive brain reading, it is really no more than reading a person’s other involuntary reactions—sweaty palms, stuttering speech, glances cast to the side—that interrogators rely upon all of the time. It may be that rather than prohibiting the collection and analysis of brain signals by the police, our society allows this behavior but sets limitations on the evidentiary value of the information collected in this fashion, and/or that courts require a warrant to use brainspray capturing technology.

Under the Katz test of reasonable expectation of privacy, we would currently be reasonable to expect that the thoughts inside our heads would be private. Katz v. United States, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967). But the Katz test allows for changes in social norms. For example, it may soon be unreasonable for U.S. citizens to expect behavioral privacy anywhere but in their own homes, given the expansive systems of cameras, drones, and satellites available to watch their every move. Similarly, it may soon be unreasonable to expect that U.S. citizens can expect geolocation privacy anywhere at all, given that smartphones, cars, tablets, and other items capture and report location data constantly. So it is not outside the realm of belief that one day brain scanning and reading technology will become pervasive enough that it would be unreasonable for a person to believe that he or she were not open to a scan while standing in a public place, or stopped in a car at a traffic signal.

One of the most intriguing questions is whether the invasion of a person’s thoughts ever will be considered a criminal act in this country? We have been discussing passive capture and interpretation of brain signals, which could, in itself, be considered an assault on the victim whose brain was mined for data. Assault has traditionally been both a crime and a tort, and it consists of a threat against a person combined with the present ability to act on that threat. Battery, on the other hand, involves a touching of a person and harm resulting from that touch. Battery also supports both civil and criminal penalties. The field of brain signal research and practical applications show us that brain crimes could be possible even given the technology available or under consideration right now. For example, actively forcing signals into a person’s brain without that person’s permission can be a sort of “brain rape,” especially if the victim is made to act involuntarily as a result of the imposing signals. It is easy to imagine the use of a special helmet by the military that is capable of affecting brain health with a transcranial magnetic or ultrasonic stimulation device, so that a hack of that helmet could cause damage to the brain health of the soldier wearing it or could force the soldier to take an action against his or her interest or to forgo an action in that interest. The physical effect would not have to be overwhelming to be significant.

If the helmet simply made a soldier stand still for a moment in a foxhole or hiding position, it could cause the ultimate damage. If it caused a pilot to sleep for a moment at the controls of an aircraft, the worst would occur. Such an act would meet all the elements of a crime, and could be harmful, perhaps even fatal, to the victim.

There are commercial legal issues of this technology as well. For example, a company that develops a prosthetic limb that is connected directly to the nervous system of its wearer would want to own the data generated by the computing aspects of the device. This data will be helpful in servicing the limb and in developing better subsequent prosthetics. But can we allow a company to own the interior directed thought signals of the wearer and to know the thinking process that is encompassed in each action of the limb? Data ownership of brain signals and intellectual property claims on active thoughts will open a new area of consideration for commercial exploitation of personal data. It is one thing to allow the grocery store to keep records of all that you purchase there, and another thing altogether to allow a private company to own the signals sent from your brain to your right hand.
**Conclusion**

Is reading or manipulating the brain from outside a person’s head a legal bright line, or will we have time to grow accustomed to the practice before the law addresses it? Without a doubt, the dawn of brain signal capture and interpretation is upon us, and like other technologies in our lives, it will continue to grow in usefulness and relevance until we are all acclimated to it. We should consider the legal and ethical consequences of such technologies now, so that we are not forced to do so when the technologies and the legal implications affect us all.

Theodore F. Claypoole is a partner at Womble Carlyle Sandridge & Rice, LLP, in Charlotte, North Carolina.
Revisiting the Public Performance Right in the Battle Over Broadcast

By Jon M. Garon

A multitude of new technologies has changed the way in which broadcast television signals can be transmitted to viewers. Aereo, Inc., provides its paid subscribers the ability to receive local television signals directly over the Internet. It provides this service in areas of New York, Boston, Atlanta, and a growing list of other cities. Aereo uses micro-antennas housed in its own facility to receive the signal locally and then retransmits that signal to the subscriber using the Internet. Under the Aereo confirmation process, a customer must have a credit card with a valid billing address in the city where the customer wishes to enroll. So although the technology would allow for a person to use the service nationally (or even globally), the Aereo business policies focus on territorial restrictions. FilmOn X offers a similar service in other parts of the country.

At stake is the legal question as to whether the retransmission to thousands (and eventually millions) of viewers using individual antennas constitutes a public or private performance of the television broadcast. If the broadcast is entirely private, then Aereo, FilmOn X, and other Internet redistributors need no license and the television stations have no legal basis to claim the retransmission fees they would earn if the subscribers watched through a cable provider.


To many, this may be an arcane debate over vestigial technologies. Approximately 82.2 percent of Americans no longer use television antennas, though this number dropped from 85 percent in the previous year. Today most of the public receives its broadcast television through cable retransmission. But as the small dip in cable subscription suggests, consumers are looking to the Internet and other alternatives for their broadcast television content. Broadcasters, in turn, are looking to cable retransmission fees as an increasing source of non-advertising revenue. The recent month-long blackout of CBS on the Time Warner Cable system retransmission fees highlighted the significance of the revenue battle between broadcasters and cable systems. If Internet companies are able to avoid the licensing fees paid by cable companies, then television and sports broadcasting could be upended.

To determine the obligation to pay for the retransmission rights, the courts must define the meaning of public performance under the Copyright Act. Aereo and FilmOn X believe the one-to-one correlation between the micro-antennas and viewers means each viewer receives a private signal. Broadcasters stress that the system of micro-antennas broadcasts to the general public.

The Supreme Court answered precisely this issue under the 1909 Copyright Act. In *Fortnightly Corp. v. United Artists Television, Inc.*, 392 U.S. 390 (1968), the Supreme Court addressed the question of whether use of a distant commercial antenna to retransmit broadcast signals constituted a public performance. The Court said it did not. “If an individual erected an antenna on a hill . . . he would not be ‘performing’ the programs he received on his television set. . . . The only difference in the case of CATV is that the antenna system is erected and owned not by its users but by an entrepreneur.” The Court then extended this view to rebroadcasts in distant markets, giving rise to cable superstations and the modern cable landscape. *Teleprompter Corp. v. CBS, Inc.*, 415 U.S. 394, 94 S.Ct. 1129, 39 L.Ed.2d 415 (1974). See United
Video, Inc. v. F.C.C., 890 F.2d 1173, 1176 (D.C. Cir. 1989).

The executive branch, however, did not agree. “Even before the Fortnightly decision validated this practice against copyright claims, the FCC decided that it was an unfair form of competition.” United Video at 1177. The FCC mandated protections to protect “broadcasters from the importation into their markets of distant signals that duplicated signals to which they had purchased exclusive rights.”

Like the FCC, Congress itself intervened. Congress rejected the interpretation of the Supreme Court through specific legislative changes in what became the 1976 Copyright Act. Congress added Section 106 (4) to make “public performance” an exclusive right of the copyright holder and added the Transmit Clause to the definition of make explicit that the copyright holder has the exclusive right “to transmit or otherwise communicate a performance or display of the work . . . to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.” 17 U.S.C. §101 (2013).

In the Second Circuit decision upholding the right of the Internet provider to offer a distant signal as a service to the consumer, the philosophy of Fortnightly can be readily seen. In the decisions upholding the right to control the exclusive public performance of the broadcasts, the congressional purpose of the Copyright Act is more heavily stressed.

In WNET, Thirteen v. Aereo (Aereo), the Second Circuit begins its analysis by acknowledging that “[t]he legislative history shows that the Transmit Clause was intended in part to abrogate Fortnightly and Teleprompter and bring a cable television system’s retransmission of broadcast television programming within the scope of the public performance right.” Despite this, the Second Circuit relied on its earlier interpretation of the Transmit Clause in Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008), cert. denied, ___ U.S. ___, 129 S.Ct. 2890, 174 L.Ed.2d 595 (2009) (Cablevision). There, the court held that a licensee cable system did not need additional permission to provide a remote DVR to its customers. Importantly, it held that each separate recording and retransmission was not an additional public performance. “Each transmission of a program could be received by only one Cablevision customer, namely the customer who requested that the copy be created. No other Cablevision customer could receive a transmission generated from that particular copy.”

The Aereo opinion embraces Cablevision and extends it to its furthest possible extent. Many academics have criticized the poor statutory interpretation. Professor Jane Ginsburg, for example, highlights the failure to use the phrase “members of the public” in the analysis and to confute performance with transmission. WNET v. Aereo: The Second Circuit Persists in Poor Interpretation models and schedules – all would be adversely affected. . . . These concerns apply with equal force here.”

Also interesting in the Aereo decision are the facts not relied upon in the decision. Aereo provides a very careful business plan – unlike that of WPIX, Inc. v. ivi, Inc. – by limiting access to its local television rebroadcast to customers who have a credit card billed to the market in which the person subscribes. This local reproduction feature is not relied upon by the Second Circuit, but it provides a significant protection from claims the Aereo broadcast violates the non-duplication or exclusivity rules of the FCC. These are the rules that result in a local station having priority over a national cable broadcaster from airing the same show. By transmitting only to the audience that is technically within the market of the over-the-air broadcasters, no other broadcaster can claim to have its non-duplication rights impacted.

The geographic limitations of Aereo do not seem to be relevant to the Second Circuit. As a result, Aereo could choose to expand its coverage to a subscriber living anywhere in the country. And of course, the mailing address for a customer’s credit card bill does not necessarily equate with the ac-
tual residence of that customer. Sports fans, for example, may find the cost to acquire a P.O. box in the home of their favorite franchise is a trivial expense to then stream local broadcasts wherever the fans happen to reside.

Although the courts have arrived at very different conclusions, the D.C. District Court in FilmOn X noted that FilmOn X’s technology closely mirrors that of Aereo.

FilmOn X readily admits that its technology is “similar . . . in every relevant way” to the technology at issue in Aereo. . . . FilmOn X installs an array of “mini antennas, each no larger than the size of a dime and spaced inches apart.” A large number of mini-antennas are aggregated on a circuit board, which also contains other electronic components essential to FilmOn X’s Internet broadcast system. An antenna may be assigned to a specific individual user (“static”). More generally, an antenna is available for “dynamic” allocation by the tuner server – that is, a specific antenna is assigned to one specific individual user only when that user is watching television via FilmOn X and is assigned to a different user when the first user is done. No single antenna is used by more than one user at a single time, and all dynamic antennas are shared.

The D.C. District Court carefully reviewed the analysis of the California and New York judicial decisions before turning to the legislative history of the 1976 Copyright Act. District Judge Rosemary Collyer looked to the House Report to better understand the definition of “publicly perform” under the Copyright Act. As she noted, “[t]he House Report for the 1976 Act clarified: ‘Under the definitions of “perform,” “display,” “publicly,” and “transmit” in section 101, the concepts of public performance and public display cover not only the initial rendition or showing, but also any further act by which that rendition or showing is transmitted or communicated to the public.’”

Reviewing this section and many other similar provisions of the legislative history, the D.C. District Court found that FilmOn X performs the copyrighted works publicly when it transmits a performance of the work by means of a device. Judge Collyer found that the language of the statute compelling and that any possible ambiguity in favor of FilmOn X was decisively answered by the legislative history which explained both that the definition of “publicly perform” was to capture all possible performances and the methods were intended to capture all devices when known or later created. Given the broad sweep of congressional intent and statutory language, the court emphasized a split between the Second Circuit and Ninth Circuit on the practice of DVD rentals in hotels. In On Command Video Corp. v. Columbia Pictures Industries, 777 F.Supp. 787 (N.D.Cal.1991), a federal court in California had earlier held that a hotel provided a public performance when it played individual videotapes to its hotel rooms, even though no tape could be viewed by more than one room at a time. Since the analogy between Aereo’s transmission and that of the hotel operator was quite close, the Second Circuit declared On Command wrongly decided. But Judge Collyer noted the Ninth Circuit never rejected the On Command understanding of public performance and by extension the limitation on Aereo and FilmOn X within the circuit.

The nature of the split and the economic consequences provide a compelling case for Supreme Court review. Four circuits have made different determinations regarding the public performance rights. But the judicial branch is not the only voice to be heard. The Department of Commerce has added a cautionary voice on the subject. In a July 2013 green paper on copyright, the Department of Commerce Internet Policy Task Force addressed the developing Aereo case law. Copyright Policy, Creativity, and Innovation in the Digital Economy, Dept. of Comm. Internet Policy Task Force, July 2013, www.uspto.gov/news/publications/copyrightgreenpaper.pdf.

Courts are grappling with this issue and it remains to be seen how it will be resolved. And while the answers may require careful parsing of statutory language and legislative history, the underlying policy question is which businesses will benefit to what extent from new technologies that meet the consumer’s desired enjoyment of content. The result of these cases could affect, for example, the viability and scope of new licensed business models such as online video subscription services. To the extent that judicial decisions undermine a meaningful public performance right, Congressional action may be needed.

The last sentence of the Commerce Department review emphasizes that Congressional action may be needed if the public performance right is undermined. The statement appears to suggest the Department of Commerce prefers the position of the broadcasters, but only to the extent consumer interests are also taken into account. Under this reading, the green paper might be suggesting that Internet retransmissions require a license but also that any license should include the convenience and services extracted under Cablevision. Whether such a balance can be found through a court decision is unclear. As with Fortnightly and Teleprompter, it is likely the final word will be that of Congress.

Reading the advice by the Department of Commerce that public performance rights may require new balancing, the Supreme Court may prefer to leave this controversy among the list of topics for Congress to address when it tackles copyright reform more broadly. Moreover, given the intersection between copyright and FCC regulation which addresses non-duplication rules and other policies not properly before the Court, the Supreme Court could well defer any decision on Aereo to Congress.

Whether the conflict is reviewed at the
Supreme Court or on Capitol Hill, the delays incumbent in any decisional process will result in the growth of unlicensed Internet services and increasing opportunities for the public to “cut the cord” by leaving cable for Internet television reception. The imperative by cable companies to reverse this trend and the greater ability to control Internet retransmission may shift more original content to cable channels and away from broadcast channels. Broadcast television remains highly lucrative, but the opportunity to control broadcast exclusivity through cable may make the cable stations the primary source of content in the future.

The result of this shift would be a further disenfranchisement of the minority of viewers who rely on free television through the public airwaves. It would also shift economic power to the content distributors because the cable operators would get less value for their rebroadcast fees. The shift would undoubtedly create an opportunity to increase consumer costs for television content but increasing competition from non-broadcaster content and the fragmentation in the television marketplace would be strong countervailing pressure to remain price competitive.

Ultimately, the split between the courts on the meaning of “publicly perform” copyrighted works must be resolved and the judicial resolution is likely only the backdrop for legislative reform. The process, however, will be lengthy. The changes to broadcaster’s reliance on over-the-air transmissions as their first run venue of choice may permanently shift well before the conflict is resolved.

Jon M. Garon is Director, NKU Chase Law + Informatics Institute and Professor of Law, Northern Kentucky University Salmon P. Chase College of Law.
In 2012, wanting to assist small businesses and boost job creation, Congress enacted the JOBS Act. Part of the act requires the Securities and Exchange Commission (SEC) to adopt rules to exempt crowdfunding offerings from registration under the securities laws. On October 23, 2013, the SEC issued its long-awaited rule proposal on crowdfunding, bringing it one step closer to fruition.

Crowdfunding means different things to different people. Crowdfunding, crowd-sourcing, and general solicitation in private offerings all seem to be mixed together when people talk about crowdfunding. The SEC’s recent rule proposal may seem confusing because many appear to already be involved in crowdfunding. To clear up any confusion and to help explain the SEC’s rule proposal, the following briefly explains the current state of crowdfunding.

**What Is Crowdfunding?**

First, the SEC is involved only with securities-based crowdfunding. If anyone sells securities, they must register the transaction with the SEC or have an exemption from registration. Securities-based crowdfunding will be one of these exemptions when the SEC adopts the new rules.

Other forms of capital-raising are often called crowdfunding, but there are important differences under the securities laws.

Second, some intermediaries currently “crowdsource” funds for a variety of projects using donation-based crowdfunding, but the funding recipients do not issue securities in exchange for the money received, thus remaining outside the reach of securities regulation. Examples include Kickstarter, Indiegogo, GoFundMe, and RocketHub. Although donors do not get securities, they often get rewards for their money, such as a product of the company, a t-shirt, tickets to an event, etc.

Finally, some intermediaries currently provide a web-based platform for issuers to connect with “accredited investors” in unregistered securities offerings, usually under the exemption for private offerings in Section 4(a)(2) of the Securities Act of 1933 (the Securities Act). This medium was expanded when Rule 506(c) of Regulation D went into effect in September 2013, permitting general solicitation and advertising in some unregistered offerings. Typically, broker-dealers licensed by FINRA – and regulated by the SEC and FINRA – operate these capital-raising websites, and only accredited investors may invest in these companies.

**The SEC’s Crowdfunding Rule Proposal**

The crowdfunding exemption proposed by the SEC, in accordance with the mandate in the JOBS Act, will provide a securities-based option in addition to the donation-based crowdfunding options already in use. Generally, under the proposed exemption, investors will receive securities in exchange for their capital contributions, and non-accredited investors may participate in the crowdfunding offerings. To implement the new program, the SEC’s proposed rules, to be known as “Regulation Crowdfunding,” impose a number of requirements on issuers and the “funding portals” that will host crowdfunding offerings. Here are some of the notable provisions of the proposed rules:

**Proposed Limits and Key Requirements**

- Issuers may raise a maximum of $1 million annually under the crowdfunding exemption.
- The aggregate amount sold to any investor under the crowdfunding exemption in a 12-month period cannot exceed:
  - The greater of $2,000 or 5 percent of the annual income or net worth of the investor, if either the annual income or net worth of the investor is less than $100,000; and
  - Ten percent of the annual income or net worth of the investor, not to exceed the maximum aggregate amount of $100,000, if either the annual income or net worth of the investor is $100,000 or more. The annual income and net worth amounts are calculated according to the rules used to determine annual income and net worth for accredited investors. This means that the investor’s primary residence will be excluded from the calculation and the investor’s annual income and net worth may be calculated jointly with that of a spouse.
of the investor’s spouse.

• A securities transaction under the crowdfunding exemption must be conducted over the Internet through a broker or “funding portal.”
• The proposed rules exclude certain issuers, including issuers without a specific business plan, registered public companies, foreign issuers, investment companies, and hedge funds.
• Securities purchased in a crowdfunding offering are subject to restrictions on resale for one year.
• Advertising of crowdfunding offerings is limited to notices similar to tombstone ads permitted under Securities Act Rule 134.

Proposed Disclosure Requirements

Issuers are required to disclose in filings with the SEC the following items, among others:

• Shareholders holding more than 20 percent of the issuer’s total outstanding voting securities;
• The current business and the anticipated business plan;
• Financial condition;
• Use of proceeds;
• Target offering amount, deadline to reach the target offering amount, and regular updates regarding the progress toward the target offering amount;
• Price of the securities and the method used to determine the price;
• Ownership and capital structure;
• Risk factors;
• Related-party transactions, since the beginning of the issuer’s last full fiscal year, in excess of 5 percent of the amount of capital raised under the crowdfunding exemption during the preceding 12 months; and
• Compensation paid to the intermediary.

The proposed rules require financial statements prepared in accordance with U.S. GAAP, covering the shorter of the two most recently completed fiscal years or the period since inception of the business. The level of financial disclosure depends upon the size of the offering:

• Issuers offering $100,000 or less:
  • Income tax returns filed by the issuer for the most recently completed year and financial statements certified by the principal executive officer.
  • Issuers offering more than $100,000 but not more than $500,000:
    • Financial statements reviewed by an independent public accountant.
  • Issuers offering more than $500,000:
    • Audited financial statements.

After an issuer sells securities under the crowdfunding exemption, annual reports must be filed no later than 120 days after the end of the most current fiscal year covered by the report. Issuers must continue to file annual reports until:

• The issuer becomes a reporting company under the Securities Exchange Act of 1934;
• The issuer or another party purchases or repurchases all of the securities issued in crowdfunding offerings; or
• The issuer liquidates or dissolves its business in accordance with state law.

Issuers may not be eligible for additional crowdfunding offerings if they have not met their annual reporting requirements during the two years immediately preceding the new offering.

Proposed Bad Actor Disqualification Provisions

Issuers, officers, directors, general partners, managing members, 20 percent beneficial owners, promoters, and compensated solicitors are all subject to “bad actor” disqualification provisions. Disqualifying events include felony and misdemeanor convictions for securities fraud in the last 10 years, securities-related injunctions or court orders within the last 5 years, and certain SEC orders. The disqualification provision will require extra diligence from issuers to ensure that covered persons have not had a disqualifying event that would make the issuer ineligible for the crowdfunding exemption.

Funding Portals

A funding portal is any person acting as an intermediary in a transaction involving the offer or sale of securities for the account of others, solely pursuant to the crowdfunding exemption, that does not:

• Offer investment advice or recommendations;
• Solicit purchases, sales or offers to buy the securities offered or displayed on its platform or portal;
• Compensate employees, agents, or other persons for such solicitation or based on the sale of securities displayed or referenced on its platform or portal;
• Hold, manage, possess, or otherwise handle investor funds or securities; or
• Engage in such other activities as the SEC determines appropriate.

FINRA has also issued proposed rules for funding portals and broker-dealers who will participate in crowdfunding offerings.

Conclusion

The proposed crowdfunding rules impose substantial requirements on issuers. Prior to deciding to pursue a crowdfunding strategy, we suggest that business owners consider the requirements that the SEC has proposed to impose on crowdfunding offerings and discuss with their advisers the impact and costs of these requirements.

The proposed crowdfunding rules provide an exciting new opportunity for fundraising and may provide a good source of capital for the right issuers. Since the crowdfunding rules are only proposed rules, they are still subject to public comment and revision by the SEC prior to adoption. If parties would like to weigh in on the SEC’s proposed rules, they can submit comments on the proposed crowdfunding rules to the SEC within 90 days from the date the rule proposal is published in the Federal Register, which is expected to occur shortly.

Eric R. Smith is a partner and member of Venable LLP’s Corporate Transactions and Finance Group in Baltimore, Maryland. Parker B. Morrill is an associate in Venable’s Corporate Group at the firm’s Washington, D.C., office.
The number of initial public offerings in 2013 is up sharply over that of 2012. Approximately 85 percent of U.S. IPOs in 2013 involved Delaware corporations. Some of these IPO companies were originally incorporated outside of Delaware, but reincorporated into Delaware in anticipation of their IPO.

Given the predominance of Delaware as the jurisdiction of incorporation for IPO companies, Delaware law plays a significant role in IPOs, as it does in M&A transactions. However, the relevant Delaware issues are somewhat different. In M&A transactions, the focus is typically on the terms of the merger agreement and the fiduciary duties of directors. In IPOs, the focus is more likely to be the company’s historic capital structure and the terms of its charter and bylaws. There are several issues to watch out for.

Problems with Pre-IPO Capital Structure Can Infect the IPO

A key aspect of IPO diligence is reviewing the company’s pre-IPO capital structure. This requires scrutiny of the board and stockholder actions approving such matters as prior stock issuances and option grants, and the filings made in Delaware to effectuate them (e.g., charter amendments or certificates of designation creating preferred stock for a financing round). It will also often require checking that the company’s directors had been properly elected.

Problems may arise for two main reasons. First, such diligence requires looking back to the earlier stages of a private company’s life, when attention to corporate formalities and record keeping may not have been as careful as during the build-up to an IPO. Second, the rules of Delaware law that apply to such early-stage actions are quite strict. In fact, Delaware cases have made clear that failure to adhere to such rules may render the actions in question void or voidable. Cases have applied this reasoning to actions such as issuing stock when the board resolutions approving the issuance were not properly adopted (for example, because a written consent was not returned by all directors, or because the board had not been properly elected); effectuating a stock split without proper language in the charter or board resolutions; failing to follow the statutory sequence for charter amendments and mergers, which requires that the stockholder consents approving such matters be obtained only after the board has approved the matter; and failing to ensure that stockholder consents were signed, dated, and returned in accordance with the exact requirements of the Delaware consent statute.

The implications of such problems are not merely hypothetical. In a recent case involving Vitacost.com, Inc., the board discovered problems with the company’s pre-IPO stock issuances more than a year after the company went public. Kloss v. Kerker et al., C.A. No. 018594XXXXMB (Fla. 15th Dis. 2011). The problems stretched back to the company’s original incorporation 14 years ago, and included defects in the election of the company’s initial board of directors, as well as in the approval of certain prior stock issuances and stock splits. After an investigation by its audit committee, the company restated its financials and faced delisting from Nasdaq. It also faced stockholder derivative suits, which it ultimately settled. Such suits are often preceded by a stockholder demand to inspect the corporate records of prior transactions under Section 220 of the Delaware General Corporation Law (DGCL), which provides stockholders with a tool to discover prior problems. The company ultimately brought suit against its corporate counsel, which had rendered an unqualified legal opinion that the company’s shares were duly authorized and validly issued.

Fortunately, while it is the strictness of certain Delaware rules that can lead to such dire consequences, Delaware law also offers several fixes. For example, Delaware law generally recognizes a broad application of the doctrine of ratification, which may enable a board to ratify and effectively cure prior stock issuances or option grants that did not previously receive proper approval. The Delaware correction statute (Section 103(f) of the DGCL) also gives a corporation the ability to correct prior corporate filings – for example, a charter amendment creating stock or effectuating a stock split – if there were errors in such filings. If these fixes are not available under a given set of facts, the corporation may be able to effectively reissue improperly issued stock if certain steps are taken before...
the IPO.

In addition, partly in recognition of the threat that Delaware’s strict rules can pose to a successful IPO, the DGCL was amended this summer to adopt two new sections allowing corporations to validate prior acts, such as stock issuances, that might otherwise be invalid under Delaware case law. New Section 204 of the DGCL allows a corporation to cure prior defects without going to court. New Section 205 allows a corporation to seek judicial validation of prior defective acts. Both sections effectively require a “redo” of the act in question by the board or stockholders, as applicable, as well as notice to stockholders. Generally, if no stockholder objects within 120 days, then the act in question is no longer subject to invalidation based on prior defects in authorizing the act. Importantly, however, while Sections 204 and 205 were adopted this year, they do not actually take effect until August 1, 2014.

Charter and Bylaw Issues

In connection with going public, most companies amend their charter and bylaws to adopt various provisions that are more typical for public companies than for private companies. In addition, typically, the company’s pre-IPO preferred stock would be converted to common stock, and going forward the company would have only common stock outstanding (although it might have preferred stock authorized in its charter, most likely pursuant to a “blank check” provision allowing the board to fix the terms of such stock).

Interestingly, while most existing public companies have had to back off of their anti-takeover provisions in recent years – for example, by eliminating classified board structures (under which directors serve three-year terms and are only removable for cause) and implementing majority voting for directors (instead of traditional plurality voting) – new IPO companies are much more likely to retain these and other anti-takeover features. Thus, counsel will need to assess the desirability of various charter provisions that are available under Delaware law – including a classified board, elimination of the stockholders’ right to act by written consent, blank check preferred stock, supermajority vote requirements in the charter and bylaws, advance notice bylaws, voting standards in director elections, and the applicability of Section 203 of the DGCL (Delaware’s anti-takeover statute).

Companies will also have to decide whether to adopt certain “state of the art” bylaw provisions, including:

Exclusive Forum Provisions

These generally provide that any stockholder lawsuit relating to director fiduciary duties or compliance with Delaware corporate law must be brought only in Delaware. Such bylaws were upheld in a much-noted decision this summer involving Chevron and FedEx. Boilermakers Local 154 Ret. Fund v. Chevron Corp., C.A. No. 7220-CS (Del. Ch. June 25, 2013); see also Edgen Grp. Inc. v. Genoud, C.A. No. 9055-VCL, (Del. Ch. Nov. 5, 2013)(Trans.). Many public companies and companies doing IPOs responded by adopting such bylaws. However, that response has been far from universal, in part due to uncertainty concerning the reaction of proxy advisory firms such as ISS and Glass Lewis. The decision of any particular company on this issue may depend in part on the presence or absence of certain other features in its charter or bylaws. For example, if a company is not subject to majority voting for directors, then a “vote no” campaign against reelection of a board would be less of a threat than for an established public company that was subject to majority voting.

Indemnification

Most public Delaware corporations provide some degree of indemnification coverage in their charter or, more typically, bylaws. However, some companies have begun to rethink boilerplate forms that require full indemnification and advancement of defense costs in all cases. For example, Goldman Sachs recently was required to pay the defense costs of a computer programmer of one of its subsidiaries who was prosecuted for stealing Goldman’s computer code. Aleynikov v. Goldman Sachs Group, Inc., 2013 WL 5739137 (D.N.J. Oct. 22, 2013). The reason was a broad, boilerplate bylaw requiring full indemnification and advancement of expenses for “any officer” of the firm or its subsidiaries. Largely because the programmer had the title of “vice president,” the court ruled that he was entitled to coverage (notwithstanding Goldman’s argument that “vice president” was a widely used “courtesy title” and that the person in question did not exercise any typical managerial or officer functions, which was not disputed). Goldman also was required to pay the litigation costs incurred in suing Goldman to enforce the bylaw. One takeaway for companies contemplating an IPO is to assess the scope of boilerplate indemnification grants, and in particular which officers and employees will fall within the coverage (both at the parent company and subsidiary level).

Director Qualification Bylaw

IPO companies may also consider whether to adopt a new bylaw designed to disqualify director candidates who receive compensation from insurgent stockholders, such as candidates who agree to serve on a hedge fund’s proxy contest slate. There have been a few high profile adoptions of this bylaw by established public companies, such as Marathon Oil and Halliburton (modified version). However, the Delaware courts have not ruled on the validity of such a bylaw.

Finally, companies that choose to reincorporate into Delaware prior to an IPO will often want their new Delaware charter to carry forward the rights of stockholders that existed under the pre-Delaware charter, including accrued dividends (which often add on to a preferred stock’s liquidation preference) and conversion adjustments. This may require careful drafting to preserve such rights rather than simply duplicating all the terms of the prior charter.

Jeffrey R. Wolters is a partner at Morris, Nichols, Arsht & Tunnell LLP in Wilmington, Delaware.
Ethics Corner
Our New Column; and the “No Contact Rule”

By Robert Evans III

Continuing in the tradition of Bill Freivogel’s columns (see the Business Law Section’s “eSource”: Oct. 2007, Volume 6, No. 2 to Nov. 2009, Volume 7, No. 12), “Ethics Corner” will appear every other month in Business Law Today. The goal of this column will be to present topics that occasionally confront lawyers, principally business lawyers, involving the ethics rules. Not all of the columns will be specifically limited to ethics; we hope to touch on professionalism and civility as well from time to time. One issue that may become apparent is that the ethics rules are written with litigation in mind and may not always fit smoothly with a typical corporate, securities, or transactional practice. In that light, this column will attempt to emphasize the everyday over the esoteric and to alert business lawyers to topics they should be sensitive to without providing an in-depth academic analysis or answering all of the questions raised.

Ethics issues arise in specific fact patterns, so we’ll start with a hypothetical:

Andy, a New York corporate and securities lawyer, had just finished one meeting and was preparing for the next when one of his banker clients, Gus, called. Gus explained that he and his team were meeting with the CEO and CFO of a mid-market company later that day to talk about going public. Gus told Andy that the management team is very detail oriented, and would Andy be available to get looped into the meeting if they got past the high-level discussion and into the weeds? Andy asked what kinds of things Gus thought he might need to address. Gus said he’d want Andy to cover any SEC rules that came up and that the CEO and CFO were likely to be focused on disclosure about management compensation, limits on insider sales in the offering and after, publicity restrictions, timing, and expected costs.

The first question is whether any ethics rules are implicated by this fact pattern. What should Andy be alert to?

Questioning Participation in the Meeting

The title of this column has probably flagged one potential issue: can Andy participate in the meeting if the company’s lawyer is not present?

Business lawyers are used to sophisticated businessperson clients, some of whom may know more law relevant to their business than the lawyer does and may readily agree to meet with lawyers for the other side of a transaction without their lawyer present. They will have time to check with their lawyer before any binding commitments are made.

Back to our hypothetical:

Andy asks Gus if the company’s lawyer will be at the meeting. Gus says, no, just the CEO and the CFO. Gus does not know whether the company has engaged lawyers for an IPO and is not entirely sure whether the company has a general counsel. Andy explains that, for him to participate, the company’s lawyer should be on the phone as well. Gus checks with the CEO, who says that their general counsel is not available and that it would be great if Andy can participate because he has lots of detailed questions about the process.

The New York ethics rules, similar to the ABA Model Rules, govern communications with persons represented by counsel (Rule 4.2 – often referred to as the No Contact Rule). (See sidebar below for language of Rule and Comments.)

The ethics rules regarding communicating with other parties have a fair amount of nuance to them. There are over 50 pages in Simon’s New York Rule of Professional Conduct Annotated on Rule 4.2 alone.

In our hypothetical, some of the trickier issues – like whether a litigator can talk to employees of a defendant corporation – fall away. Andy would be talking directly to senior management.

Further Issues

Some issues remain:

• Can we read the term “party” narrowly to apply only to litigation?
• If the company is represented by outside counsel, can Andy talk to the general counsel instead?
• Can the client waive the No Contact Rule?

The term “party” gets read more like “person” in the context of transactions by the New York State Bar Committee.

Whether a company having a general counsel means that it is always a person represented by counsel raises some interesting questions. The New York City Bar Association Formal Opinion 2007-01 discusses some of the contours of situations involving general counsel and makes it
clear that if the general counsel is acting as a lawyer for the organization (and not merely as outside counsel’s client) then the communication is permitted.

Because the CEO is prepared to waive the need for his lawyer to be in the meeting, it is tempting to think that Andy can participate. However, Rule 4.2 requires “prior consent of the other lawyer” unless the communication is otherwise authorized by law.

Andy may speculate about whether he is really “representing a client” and communicating “about the subject of the representation.” He might argue that, until the bankers win a mandate, all they are doing is talking about how the law works and how IPOs are done and he is marketing his services as a potential underwriters’ counsel. Andy should consider though, how his participation in the meeting might appear, assuming Gus and his team get hired to do the deal and they hire Andy. Only after the deal moves forward and a problem develops with a topic that Andy discussed at the meeting will the ethics question present itself. In that situation, it may be difficult to defend Andy’s reasons for participating.

Andy still has a chance to escape any ethics issue. If he can get in contact with the general counsel and get permission to meet with the CEO and CFO without counsel present, then he will have met his ethics obligations under Rule 4.2. That may be easier said than done. Andy’s client is unlikely to want Andy to reach out directly, and the CEO seems to have dismissed the issue.

Conclusion

A business lawyer invited to help out at a meeting between bankers and a company they are working with (or are pitching) can be in a tough spot ethically. Rule 4.2 – the No Contact Rule – may prohibit the lawyer from participating in the meeting without prior consent of the company’s counsel unless company’s counsel participates as well.

Robert Evans III is a partner at Shearman & Sterling LLP in New York.
Good things happen when lawyers help out. I have had the pleasure for the last 18 years of working with a group of lawyers, court and law office staff, and financial professionals with a program called CENTS (Consumer Education and Training Services). While I am frequently referred to as the co-founder of CENTs, the other co-founders were local bankruptcy attorneys who believe as I do, and did then, that with better community-based education on how to use credit wisely, we can reduce the business of the bankruptcy courts, where we as bankruptcy professionals see only the sad consequences of personal and commercial financial collapse.

When CENTs was born in 1995, we were an ad hoc group of bankruptcy judges and lawyers who were soon joined by clerks’ office and law firm staff and accountants and turnaround professionals. We had one goal: to improve financial literacy in our community. At that time, through the King County Bar Association, we supported a once-a-week legal clinic where low-income consumers could obtain 30 minutes of free legal advice from a trained bankruptcy attorney. We wanted to broaden our efforts to stem the never-ending flow of consumers to that clinic. Over the years, with the benefit of a number of unique alliances, CENTs has grown to be a nationally recognized provider of quality financial literacy resources for adults and teens, with a full-time, paid executive director.

When our executive director, Tony Lea-hy, joined CENTs, things really took off. With his vision, energy, and many talents in addition to legal talents, in particular his degree and expertise in film and video, he has guided CENTs for over 10 years. Our first unique alliance was with the King County Bar Association, which agreed to treat Tony as one of its employees, providing him with salary and benefits, as long as the newly incorporated nonprofit CENTs would reimburse the association for those costs as well as CENTs’ share of any other operational costs related to its activities. That arrangement has worked well and has enabled CENTs to grow tremendously with the addition of generous bankruptcy lawyers and financial professionals who help out as officers and board members, on special projects, with fundraising, at social gatherings, and doing whatever else needs to be done. Our two annual fundraisers, a dinner dance, and a bowling tournament bring big and small firm, debtor and creditor, lawyers and accountants together to socialize and become friends.

Today, CENTs’ programs and projects reach over 5,000 people every year. In addition to its now twice-weekly specialized legal clinic, CENTs offers online and in-person money management classes, pre- and post-bankruptcy debtor counseling and education courses, and has produced two educational DVDs, \textit{Smart Borrowing}, a 40-minute educational video and workbook about making wise borrowing choices (including information on borrowing fundamentals, credit cards, auto loans, payday loans, mortgages, and mortgage refinance), and \textit{Debt Slapped}, an innovative 40-minute educational video and website created to engage high school and college students about the perils of excessive debt and the urgent need to make informed student loan and credit choices. These videos were funded by grants from the Consumer Protection and Education Fund, a longtime supporter of CENTs. In 2011, the \textit{Debt Slapped} video and website were updated to conform to changes in credit laws with grants from the Western District of Washington Bench and Bar Fund and the Washington State Department of Financial Institutions – yet another new and unique alliance. The video has been distributed to schools all over the state of Washington and elsewhere and is made available nationally on the \textit{Debt Slapped} website (www.debtslapped.org). The need is great. Since 1999, average student loan debt has increased by more than 500 percent.

In conjunction with a program called CARE (Credit Abuse Resistance Education; http://care4yourfuture.org), which was founded by a bankruptcy judge in New York, I frequently take the \textit{Debt Slapped} video and companion PowerPoint presentation with other CENTs volunteers into local area high schools to talk directly with kids about their financial future. Through another unique alliance, with Seattle University Law School, law students working with CENTs on for-credit externships have helped us improve all of our \textit{Debt Slapped} materials and this year obtained approval from the Seattle School District to create a
program for math teachers on how to incorporate financial literacy concepts into their high school math curriculum. These law school students not only study the financial laws applicable to credit cards, pay day loans, and student loans, they also learn what great legal tools they have to benefit their community.

CENTS is in the process of creating a similar video and website to address the need to protect another vulnerable population, our senior citizens, again with the support of our Bench and Bar Fund and a grant from the American College of Bankruptcy. With Tony as our movie director, volunteer lawyers and accountants are working on the Senior Money script and content which will address things like reverse mortgages, telemarketing, mail, and online scams targeting seniors. The need is great here too, as research from insurance provider MetLife has found that Americans over the age of 60 are swindled out of nearly $3 billion every year.

Indeed, good things happen when lawyers help out. They change their community, become more collegial, and have fun. During the financial calamity of the last few years, the professionals and staff who generously give of their time to CENTS have come through one of the most hectic periods of their professional careers. Despite their huge workloads, their support for CENTS and their desire to address the critical need for financial learning resources in their community has never waned. That’s why I’m proud to work with and champion this group of dedicated professionals and staff.

Judge Karen A. Overstreet was appointed as a United States Bankruptcy Judge effective January 3, 1994, and she sits in the Western District of Washington at Seattle. She is a Judicial Liaison to CENTS and sits on the Judicial Advisory Board of CARE. In 2012, Judge Overstreet was awarded the Difference Maker Award for Community Service by the ABA GP Solo Division for her work with CENTS.
Inside Business Law:
Highlights of Committee Work Product

Late October and early November saw three great committee meetings by the LLC’s Partnerships and Unincorporated Entities Committee, the Business Bankruptcy Committee, and the Banking Law Committee. Materials from all of those meetings are available through the ABA website.

The 2013 LLCs Institute
The LLCs, Partnerships and Unincorporated Entities Committee, chaired by Thomas Rutledge, held the Second Annual LLC Institute on October 17 and 18, 2013, in Arlington Virginia. The two-day Institute featured numerous panels addressing key issues related to alternative entities and discussing the relationships between corporations and alternative entities. The keynote speech of the institute, by Chief Justice Myron T. Steele, addressed the “Growing Importance of Alternative Entities as Compared to Corporate Structures.” Here are some of the highlights of the Institute:

LLC Interests and Securities Law
Jennifer Johnston, Anita Krug, and Tanya Durkee Urbach presented the panel “LLC Interests and Securities Law” (video). The panel discussed when LLC membership interests may be considered securities under federal or state securities laws, how to avoid that designation when drafting, and the securities law implications of the default provisions of various LLC statutes.

Partnership and LLC Reorganizations
Bradley Borden, Steve Schneider, and Brian O’Connor presented the panel “Partnership and LLC Reorganizations” (video), discussing how to manage tax issues facing partnerships or LLCs in reorganizations and how to head off those issues in drafting the entities’ governing documents.

Rationalizing Entity Law: Corporate Law and Alternative Entities
“Rationalizing Entity Law: Corporate Law and Alternative Entities” (video), presented by Joan Heminway and Mark Lowenstein, addressed the theoretical and policy underpinnings of the distinct statutory frameworks for various types of business entities in an attempt to identify and rationalize the salient differences in treatment among various types of entities.

The Business Bankruptcy Committee Meeting
The Business Bankruptcy Committee, chaired by Patricia A. Redmond, held its 2013 Annual Meeting in Atlanta, Georgia, from October 30 through November 2. In addition to numerous working subcommittee meetings, the Committee presented 11 CLE programs on a wide variety of topics of interest to business bankruptcy practitioners. The materials from those programs, including audio recordings of several of the panels, are available through the Section’s website. A few highlights are the following:

Priority of Payment Issues in Chapter 9 Cases: Who Gets Paid First?
Gary Klausner moderated “Priority of Payment Issues in Chapter 9 Cases: Who Gets Paid First?” a panel of Hon. Frank J. Bailey, Jeffrey B. Ellman, and Michael J. Gearin, discussing competition between pension obligations and capital market creditors for a municipality’s funds in a Chapter 9 case.

Valuation: Challenging Legal and Factual Issues
Susan M. Freeman and Michael Reed co-moderated a panel discussion, titled “Valuation: Challenging Legal and Factual Issues” (audio), among Ronald F. Greenspan, Frank Lorincz, Hon. Bruce A. Markell, and Jeffrey Stoops, discussing recent case law affecting valuation of collateral. The panel addressed the valuation of low-income housing developments, causes of action, securitized mortgages, and brownfields, among other issues.


The Banking Law Committee Meeting
The Banking Law Committee, chaired by William F. Kroener, III, held its 2013 Annual Meeting in Washington, D.C., from November 7 through 9. The meeting fea-
tured a keynote speech by Tim Mayopoulos, the CEO of Fannie Mae. In addition, the Committee presented seven CLE programs on new and evolving topics in banking law. All of the program materials from the 2013 Banking Committee Meeting are available through the Committee’s website. Some of the highlights of the panels are as follows:

**A Look Inside the CFPB**
Meghan Musselman moderated the panel, “A Look Inside the CFPB,” (audio) consisting of Ron Rubin and Andrew Miller. The panel addressed the genesis of the CFPB, its position relative to other related agencies, and the CFPB’s recent activity.

**In-House General Counsel Panel**
The “In-House General Counsel Panel” (audio), of John Finneran, Gerald Hurst, and Berit Block, moderated by Heather Koenig, discussed the challenges facing bank general counsel in the post-Dodd-Frank-world. The panel touched on key issues related to managing relationships, sources of increasing risk, and heightened governance expectations, among other things.

**View from the Hill**
“View from the Hill” (audio), was a panel of Andrew Olmem, Sam Woodall, and Tara Foscano, moderated by Eli Peterson, which provided insight into Congress’s legislative priorities with respect to financial services.

**Agency General Counsels Discussion**
Heather Koenig, Megan Musselman, and Eli Peterson co-moderated a panel of Scott Alvarez, General Counsel FRB; Richard Osterman, Acting General Counsel, FDIC; Daniel Stipano, Deputy Chief Counsel, OCC; and Stephen VanMeter, Deputy General Counsel, CFPB. The “Agency General Counsels Discussion” (audio) for 2013 focused on the most critical issues facing the banking agencies, as seen through the eyes of the agencies’ general counsel and also addressed recent interpretive letters, rule-making, and enforcement actions.
# Business Law Today Board Members 2013–2014

## Co-Chairs:

<table>
<thead>
<tr>
<th>Warren E. Agin</th>
<th>William D. Johnston</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swiggart &amp; Agin, LLC</td>
<td>Young Conaway Stargatt &amp; Taylor, LLP</td>
</tr>
<tr>
<td><a href="mailto:wea@swiggartagin.com">wea@swiggartagin.com</a></td>
<td><a href="mailto:wjohnston@ycst.com">wjohnston@ycst.com</a></td>
</tr>
</tbody>
</table>

## Advisor:

<table>
<thead>
<tr>
<th>Robert Boehm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steiner Leisure Limited</td>
</tr>
<tr>
<td><a href="mailto:bobb@steinerleisure.com">bobb@steinerleisure.com</a></td>
</tr>
</tbody>
</table>

## Members:

<table>
<thead>
<tr>
<th>Miriam R. Albert</th>
<th>Lisa R. Lifshitz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hofstra University School of Law</td>
<td>Torkin Manes LLP</td>
</tr>
<tr>
<td><a href="mailto:lawmra@hofstra.edu">lawmra@hofstra.edu</a></td>
<td><a href="mailto:llifshitz@torkinmanes.com">llifshitz@torkinmanes.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Katherine Simpson Allen</th>
<th>Kathleen S. McLeroy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stites &amp; Harbison, PLLC</td>
<td>Carlton Fields</td>
</tr>
<tr>
<td><a href="mailto:katherine.allen@stites.com">katherine.allen@stites.com</a></td>
<td><a href="mailto:kmcleroy@carltonfields.com">kmcleroy@carltonfields.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mitchell L. Bach</th>
<th>Bradford K. Newman</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eckert Seamans Cherin &amp; Mellott, LLC</td>
<td>Paul Hastings LLP</td>
</tr>
<tr>
<td><a href="mailto:mbach@eckertseamans.com">mbach@eckertseamans.com</a></td>
<td><a href="mailto:bradfordnewman@paulhastings.com">bradfordnewman@paulhastings.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Michael St. Patrick Baxter</th>
<th>Michael K. Reilly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covington &amp; Burling LLP</td>
<td>Potter Anderson &amp; Corroon LLP</td>
</tr>
<tr>
<td><a href="mailto:mbaxter@cov.com">mbaxter@cov.com</a></td>
<td><a href="mailto:mreilly@potteranderson.com">mreilly@potteranderson.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lawrence A. Goldman</th>
<th>Jeffrey W. Rubin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gibbons P.C.</td>
<td>Financial Accounting Foundation</td>
</tr>
<tr>
<td><a href="mailto:lgoldman@gibbonslaw.com">lgoldman@gibbonslaw.com</a></td>
<td><a href="mailto:jwrubin@f-a-f.org">jwrubin@f-a-f.org</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Karl A. Groskaufmanis</th>
<th>Ann Yvonne Walker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fried, Frank, Harris, Shriver &amp; Jacobson LLP</td>
<td>Wilson Sonsini Goodrich &amp; Rosati</td>
</tr>
<tr>
<td><a href="mailto:karl.groskaufmanis@friedfrank.com">karl.groskaufmanis@friedfrank.com</a></td>
<td><a href="mailto:awalker@wsgr.com">awalker@wsgr.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alicia L. Gutierrez</th>
<th>Thomas W. White</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Moses Law Firm</td>
<td>Wilmers Cutler Pickering Hale and Dorr</td>
</tr>
<tr>
<td><a href="mailto:alicia@moseslaw.com">alicia@moseslaw.com</a></td>
<td><a href="mailto:thomas.white@wilmerhale.com">thomas.white@wilmerhale.com</a></td>
</tr>
</tbody>
</table>

## Editor:

<table>
<thead>
<tr>
<th>John Palmer</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABA Publishing Periodicals</td>
</tr>
<tr>
<td><a href="mailto:john.palmer@americanbar.org">john.palmer@americanbar.org</a></td>
</tr>
</tbody>
</table>