LJN LAW JOURNAL NEWSLETTERS

Cybersecurity

LAW & STRATEGY

An ALM Publication

February 2018

In This Issue:

Cybersecurity Law & Strategy

February 2018

Volume 2, Number 9

Cybersecurity Law & Strategy

Alan L. Friel
BakerHostetler
Los Angeles

Collin J. Hite
Hirschler Fleischer
Richmond,VA

David F. Katz
Nelson Mullins Riley & Scarborough LLP
Atlanta, GA

Ari Kaplan, Esq.
Ari Kaplan Advisors
New York

Justin Hectus
Keesal, Young & Logan
Long Beach, CA

Staci D. Kaliner
Redgrave LLP
Washington, DC

Dan Lear
Avvo
Seattle, WA

Kelly Lloyd
McCarter & English
Newark, NJ

Emile Loza
Technology & Cybersecurity Law Group, PLLC
Washington, DC

Ian D. McCauley
Morris James LLP
Wilmington, DE

Jeffrey D. Neuburger
Proskauer Rose LLP
New York

Nicholas A. Oldham
King & Spalding LLP
Washington, DC

Mark Sangster
eSentire
Cambridge ON, Canada

Use of the Blockchain to Contract Digitally

By Paige M. Boshell

Smart contracts are self-executing agreements written in code on the blockchain. Parties contract digitally using distributed ledger technology. This article offers a layperson's, non-technical summary of the underlying technology and consideration of certain legal implications for smart-contracting and contract management.

Blockchain Technology

The blockchain is a series of so-called "blocks": permanent files of record or transaction data. The blocks are referenced by hash pointers to form a chain sequence and the chain grows in a linear fashion over time as blocks are added sequentially using cryptography.

Picture a set of colorful plastic toddler blocks that can be connected to form various lengths of literal blockchains. These chains cannot be pulled apart, however, and blocks may not be swapped out. The chain, sequence and content of each block is permanent. Additional blocks may be added in accordance with the underlying rubric or coding of the chain. Any additional blocks are viewable by each person or entity that has access to the original chain via the blockchain platform.

Further, the blockchain may be distributed as a shared private or public database across platforms and locations. Consider a spreadsheet accessible by various parties that may view or add cells, but not revise or delete existing cells. For this distributed ledger technology, there is no centralized database to be hacked and the blocks are accessible according to permissions and visible in real time to all parties who have access to the blockchain platform.

In the blockchain, the blocks may not be removed, substituted, copied or altered. Therefore, the blockchain is considered to be inherently authenticated, secure and immutable.

Contract Process

The blockchain may be used to implement self-performing contracts. Considering again the toddler's plastic block chain, the code may be written such that if the third block is red, the fourth must be purple, but if the third block is green (or simply not red), the fourth must be yellow, and so forth. The parties agree to certain terms and outcomes to be accomplished by the contract. Using this example, the blockchain is well-suited to simple and repetitive contracts, like a series of purchases and payments. There is only one blockchain, but it is accessible from anywhere. The final terms are deployed to the blockchain and distributed throughout the underlying platform to all parties. Therefore, the contract may be executed at the same time from various locations and effectiveness can be immediate.

Further, the blockchain may be used to negotiate contract terms. The draft terms are deployed to the blockchain and distributed throughout the platform. Coding facilitates the review of contract draft terms and the sequential revision of contract documents by parties in multiple locations at the same time. Using the spreadsheet example, draft terms can be instantly viewable by all parties and the draft terms and the other party's responses and counter-terms can all be immediately logged and viewed. This allows multiple parties to negotiate and draft contracts digitally.

Contract Performance and Enforcement

The smart contract code contained in the blocks renders the contract a set of self-executing and self-enforcing protocols. If A happens, then B occurs. If A does not happen, then C occurs.

As autonomous and automated processes, smart contracts lend themselves well to agreements with clear conditions, simple terms, and repetitive transactions. These contracts may be fairly complex in terms of scope, volume and types of terms and conditions, and number of parties, but the terms must be susceptible to conversion to self-performing code.

For example, consider a sales contract. A seller of construction materials located in North America contracts with a buyer in South America. Using the blockchain, the parties could enter into the same contract at the same time. The contract protocols would provide for self-execution of the contract: the shipment of materials; the shift in risk of loss and insurability; the receipt of materials; and payment for materials. Payment can be effected digitally via the blockchain using cryptocurrency; payment and receipt would be instantaneous. If the materials are not shipped, payment is not made.

Trusted Intermediary Agreements

As an immutable and secure technology, the blockchain can be used to complete transactions typically requiring a trustee or other centralized authority to authenticate the parties, verify that certain contract terms have been met, and execute certain contract terms, such as transfer of ownership or payment.

For example, an escrow agreement can be formed and implemented on the blockchain by linking blocks of defined conditions to the release of certain payments. Independent verification of the satisfaction of the conditions is not required because the fulfillment of each condition is memorialized or effected by the blockchain. Independent disbursement of funds is not necessary because immediate transfers of cryptocurrency can be effected by the blockchain.

In this manner, smart contracts can facilitate certain types of contracts without an intermediary or trustee, at a faster pace, and at lower transactional costs than those associated with traditional trusted intermediary contracts.

Contract Management

The blockchain forms a permanent, trackable record of both the contract terms and the successful performance or failure of the contract terms. All parties have access to the blockchain — as a decentralized and distributed technology — to confirm that contract terms have been met and monitor contract performance directly.

Therefore, no separate recordkeeping or management process may be required. Blocks are accessible at any time and from any location in their permanent form. No separate method of authentication should be required. This could greatly reduce the cost of contract management, while enhancing and simplifying the administration of a vendor management program.

Traditional Contracts

As described above, the blockchain is well suited to contract terms that can be reduced to self-executing smart contract code. This requires the parties to use terms that are clearly defined, have measurable performance metrics or objectives, include concrete steps or conditions, and provide for a series of pre-determined outcomes and results.

For example, the smart escrow contract described above provides that the occurrence of specified triggers automatically and autonomously effect certain pre-determined triggered results. These escrow terms are self-executing and do not require human intervention to verify the occurrence of the triggers or effect the triggered results.

Consider, for example, a software license. Conceivably, terms governing the development of customizations according to specifications, delivery and/or installation of the software, testing and acceptance, and payments could all be memorialized, verified, and executed by smart contract code.

Traditional but more complex terms may not, however, be susceptible to realization on the blockchain. For example, the software licensee will require certain indemnities for intellectual property infringement and data breach. Determination of whether or not intellectual property infringement has occurred or claims trigger liability are not easily reduced to code. Similarly, apportionment of blame and liability for data breach may require external legal analysis. Disclaimers of warranties, limitations of liability, indemnities, force majeure, arbitration or other conflict-resolution clauses, and other so-called "boilerplate" legal terms all pose the same difficulty in this context.

Summary

In order to use the blockchain for smart contracts, the dependencies and contingencies must be expected or reasonably foreseeable, objectively measurable, and capable of concrete and automatic resolution. The protocols may be less effective for unlikely or ambiguous events or outcomes or events that require an independent legal determination to be enforced.

The efficacy of smart contracting thus depends not just on technical coding and system capabilities. The ability of the parties to foresee and define a set of terms, events, and outcomes is critical to the reduction of the contract to self-executing code. Further, the type or content of the term will impact how or whether or not the term may be suitable for the blockchain.

In the near future, use of the blockchain for smart contracts is likely to proliferate for agreements that are conducive to the technology. For more complex transactions, it will be interesting to see if these contracts will be excluded from the blockchain, effected using a hybrid approach of smart contracts and traditional contracts, or if the technology will ultimately be developed to implement these sorts of terms directly or impact the content of contract terms themselves by developing an alternative set of terms susceptible to reduction to self-executing code.

*****

Paige M. Boshell is a partner at Bradley Arant Boult Cummings LLP in Birmingham, AL. She is an IAPP Fellow of Information Privacy, Certified Information Privacy Professional/US, and Certified Information Privacy Manager. She leads the firm's Cybersecurity and Privacy, Digital Services and Electronic Contracting, and Cybersecurity and Financial Privacy teams. She can be reached at pboshell@bradley.com.

—❖—

Law Firm Security Q&A

By Adam Schlagman

With the Appleby data breach still top of mind of many law firm and legal department professionals, cybersecurity has become a major area of concern. To learn more about how law firms can protect themselves against cyber attacks and data breaches, I sat down with **Laurie Fischer**, managing director at HBR Consulting. Fischer leads the Information Governance practice at HBR, where she helps address the increasingly complex and demanding regulatory and technological challenges of today's information management environment. She has over 25 years of consulting experience partnering with clients of all industries and sizes to help them achieve their enterprise-wide and governance objectives.

Law firms are now regularly targeted by cyber criminals, most recently Appleby. Are these attacks designed to obtain specific types of information? What and why?

By their very nature, law firms maintain a higher percentage of sensitive, confidential and personal data than other industries. Most of their data also falls under attorney-client privilege, which allows clients to share highly confidential information with their attorneys without fear of it being disclosed. Law firms maintain confidential data and often sensitive information on everything from litigation case files to merger and acquisition due diligence and negotiations — and even high-profile divorce cases. This may include client Social Security numbers, medical records, intellectual property, sensitive tax and financial information, such as information on offshore transactions, as demonstrated in the Appleby case. The data maintained by a law firm is a cyber-criminal's dream! And, having access to this data can result in extortion, ransoms and exposure of highly personal and reputation-damaging information.

What are the most important steps firms should be undertaking to deter or eliminate these attacks?

It is no longer enough for a firm to simply state that their security program is ISO compliant. To help mitigate today's risks, firms must have a dedicated and active program that addresses the ever-evolving cyber risks.

Unfortunately, many firms are still taking the "wait-and-see" approach. As a result, security is not always at the top of every firm's risk management agenda. To avoid data breaches, law firms must establish the appropriate policies and procedures. For instance, firms should audit their internal processes, train employees on best practices on identifying cyber risks and set aside budget for security efforts.

That said, firms that recognize the high level of risk they face are proactive in addressing security challenges by providing the right level of funding, expertise and implementing firm-wide privacy programs. They also have established committees with representation from various departments across the firm, including IT, security, privacy, finance and HR, along with executive leadership. Firm leaders should play an integral role in establishing the correct standards and ensuring that employees are aware and trained on the risks and potential damages a cyberattack can cause. Firms must also ensure that systems are regularly updated and audit their existing programs annually, including the security practices of their third-party vendors.

To determine the maturity level of their privacy and information security practices, firms should consider a comprehensive third-party assessment of its current information security and privacy program — including its strategy, tools, technologies, processes, roles and responsibilities. After this is accomplished, the next step should be an analysis of the firm's current state against industry standards and best practices — such as ISO 27001 or the NIST Cybersecurity Framework — which will result in a gap analysis. Firms should then prioritize the cybersecurity delinquencies and develop a comprehensive action plan to close gaps in security to bolster protection. Also, firms should consider scheduling consistent testing of their security controls to ensure constant cybersecurity maintenance.

Does it make sense to prioritize certain types of clients or certain types of cases or should the same level of security be applied across the board?

Although there are certain types of cases and clients that may be more sensitive, no client would accept a substandard level of security and protection. Security measures should be consistently applied to all data and processes — no matter the client or case. This includes the implementation of measures that go beyond security-focused activities, to the appropriate

management of sensitive data, through adopting policies such as Privacy-By-Design and data governance.

What are a few less obvious solutions that firms may not have heard or considered?

Firms may consider options that remove data from their networks — and even from their data-centers. Solutions such as "air-gapping" where older, infrequently accessed data is archived to an off-network solution (and even separate location) decrease the risk of a hacker even being able to access certain data. Other options include leveraging highly secure environments provided by platforms such as Microsoft Azure and Office 365, or true infrastructure-as-a-service solutions such as Amazon Web Services. Both managed services offerings provide security options, such as MYOK (Manage Your Own Key) or BYOK (Bring Your Own Key) where the firm's data may reside on Microsoft or AWS, but the ability to access the data is controlled via encryption, and the firm manages its own encryption keys. The firm benefits from the secure infrastructure but ultimately controls who can see its data.

Should law firms be conducting preparedness exercises and unannounced tests to insure both lawyers and staff are complying with security protocols?

Unfortunately, breaches are often the fault of uninformed attorneys and staff members who have not been adequately trained on firms' security measures and privacy protocols. Before conducting preparedness exercises and tests, an important first step to ensure all employees are complying with security protocols is to roll out a comprehensive training program for all staff, with regular refreshers. This training should also be included during the new employee onboarding process. That being said, preparedness exercises and unannounced tests should still be conducted regularly as well, as they are an effective way to measure staff's understanding of all aspects of firms' security policies and procedures. Firms should also conduct tabletop exercises of their breach response plans, including response drills to emulate cyber breaches to evaluate the effectiveness of the incident response plan.

If a cyber breach is detected what are the actions that should be undertaken in the first hour, the first day and the first week?

Breach response actions and timelines should be clearly spelled out in firms' privacy and security policies. It is important for firms to have a pre-established and well-documented breach response process that addresses the steps the firm should take in the event of a data breach.

- Within the first hour, firms should focus their attention on identifying the source of the attack, initiating the breach response protocol, determining the nature of the breach and stopping additional data loss. These activities will involve action from the firm's breach coordinator, their incidence response team, internal IT and security personnel, and possibly the use of third party cybersecurity and forensics experts.
- During the first day, firms should establish appropriate communication channels, determine the nature of the breach — including its origin and target of the attack — and take the necessary steps to prevent any additional data loss. Firms also need to determine all obligations for notification of the breach, including legal, contractual and insurance requirements.
- Within the first week, firms' breach response team will need to assess the breach's overall damage to the organization, both financially and in terms of its reputation. The firm will also need to determine the best course of action moving forward, including interviewing all employees and third-party vendors with knowledge of the breach, determining notification and remediation activities, and taking necessary steps to prevent it from happening again.

*****

Adam Schlagman is the Editor-in-Chief of *Cybersecurity Law & Strategy*.

—❖—

Online Marketing Practices Continue to Pose Regulatory Threats for the Financial Services Industry

By Craig Nazzaro, Brad Rustin and Elizabeth A. DeVos

Last year, the Federal Trade Commission (FTC) released a staff report on Cross-Device Tracking, which added to the FTC's efforts to regulate emerging issues in the ever-evolving area of online behavioral advertising. The advertising in question involves the collection of data from a particular computer or device regarding a user's Internet-viewing behavior over time and across non-affiliate websites. Ostensibly, this technology obtains user preferences or interests. Cross-device tracking is the logical next step for this technology.

This cross-device tracking enables online behavioral advertising to be coordinated across a user's various devices such as smartphones, tablets, computers, game consoles and Internet-connected televisions. Using both behavioral advertising and cross-device tracking has grown since the release of the FTC study and shows no signs of stopping in 2018.

Within the guidance, the FTC acknowledges the benefits of both behavioral and cross-device tracking, but remains concerned with the privacy and consumer protection challenges raised by these systems. On the one hand, the FTC cites the benefits of a seamless experience for consumers across their devices, such as when they check email, read a book or watch a movie. Cross-device tracking also enables improved fraud detection and account security by providing companies with more options to protect a consumer by identifying a new device and requiring authentication through a known device. On the other hand, however, the FTC raises concerns over consumer transparency with the technology, particularly given that the scope of cross-device technology in this space is not understood by a majority of the public.

The Drawbacks

A large issue with both behavioral advertising and cross-device tracking is that the approach to the practice is not uniform. Vendors for financial services firms can create many different user experiences and deploy various technologies that can accomplish the goal in different ways. For example, a vendor can track a user through traditional cookies, flash cookies, Web beacons and countless other technologies, all of which may require different opt-out methods. A vendor can also positively identify the same user across multiple devices using login information or other personally identifiable information commonly called the "deterministic method."

Alternatively, a vendor can track and identify a probable user through non-personal data, such as an IP addresses. This practice is known as a "probabilistic method." As the proprietor of a website, a vendor must understand the technology and the methods being utilized by its marketing partners to properly disclose the practices and technology to the proprietor's consumers. This requires a level of due diligence that many proprietors fail to perform. Without proper controls and policies governing these practices, a website proprietor's regulatory, reputational and litigation risks all increase dramatically.

For those in the financial services industry, these leaps in technology can pose greater threats to those utilizing the services than those in less heavily regulated industries. For example, if lenders employed these technologies to capture data that contain contact information, the lenders can find themselves in violation of federal consumer protection regulations such as the Fair Debt Collections Protection Act (FDCPA), the Telephone Consumer Protection Act (TCPA), Equal Credit and Opportunity Act (ECOA), or the Dodd-Frank Act protections under the Unfair Deceptive or Abusive Acts (UDAAP) regulations.

Lenders are put under greater scrutiny regarding how they are using and storing the data collected and how these processes are disclosed to their consumers. Legal and compliance departments within lenders are often surprised at the magnitude of regulatory liability these practices can create. For example, if your advertising department has free reign to create the parameters of whom your institution is targeting for behavioral advertising, will any thought be given to the fair lending impact those choices may have? In another hypothetical, is your marketing department deploying technology that may return contact information for borrowers? If so, is your institution aware of how that data is stored and utilized? If not, the lender may be facing violations under the TCPA and the FDCPA.

Best Practices

To avoid these risks, address privacy concerns and improve consumer transparency regarding cross-device tracking and behavioral advertising, financial services industry professionals should take the following steps:

1. Be transparent about your data collection and use practices by truthfully disclosing your tracking activities. Draft and deploy both an enterprise-wide privacy policy and an online privacy policy.
2. Provide choice mechanisms that give consumers control over their data and, when you offer such choices, ensure that they are respected. To the extent opt-out tools are provided, any material limitations on how they apply or are implemented regarding cross-device tracking must be clearly and conspicuously disclosed.
3. Provide heightened protections for sensitive information, such as financial information, meaning express consent should be granted by a consumer prior to engaging in cross-device tracking on these and other sensitive topics.
4. Maintain reasonable security over the collected data. Companies should keep only the data necessary for their business purposes and they should properly secure the data they collect and maintain.
5. Create controls around which departments can unilaterally deploy third-party online marketing vendors. Many times, smaller lenders may be unaware of what their marketing departments are doing within the digital space and may be unaware of the regulatory risks these activities could create.
6. When negotiating the scope of services with digital advertising vendors, ensure that your legal and compliance partners review any change in technology or scope.
7. Review your online privacy disclosure annually to ensure the necessary updates are made to the policy.

Conclusion

With the technology that drives data collection evolving daily, the regulators of financial serves are taking notice. The best way to avoid the reputational, litigation and regulatory risks associated with this space is to: 1) fully (if not, over-) disclose your activity and technology to your consumers; 2) maintain strict controls over the deployment of the services and technology;

and 3) maintain a robust third-party vendor oversight function, which contemplates the regulatory implications that occur within the digital marketing space.

*****

Craig Nazzaro is Of Counsel in the Atlanta office of Nelson Mullins Riley & Scarborough LLP. His practice areas include Alternative Lending & Other Non-Bank Financial Services, FinTech, and Payments & Digital Commerce. **Dowse Bradwell "Brad" Rustin, IV**, is a partner in the firm's Greenville, SC, office whose practice areas include Banking & Financial Services, FinTech and Payments & Digital Commerce. **Elizabeth A. DeVos** is an associate in the firm's Greenville, SC, office. Her practice areas include Banking and Financial Services, FinTech, Consumer Financial Services, and Payments & Digital Commerce.

—❖—

Second Edition ABA Cybersecurity Handbook Reflects the Need for Greater Awareness

By Mark Sangster

As 2017 came to a close, the American Bar Association opened the next chapter in cybersecurity awareness with the release of the second edition of its *ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals*. The new edition comes nearly five years since the first edition made its rounds.

Following the 2012 formation of the ABA Cybersecurity Legal Task Force, the first edition of the handbook was a brave move to enlighten both attorneys and law firms to cyber risk, and the evolving interpretation of professional obligations to protect clients' confidentiality as the playing field moved from physical records to easily pilfered electronic documents. At the time, the FBI advised law firms about shoring up cyber defenses, as criminals considered law firms "the soft underbelly of American cyber security."

At the time, I was working with law firms to expose the risks associated with the types of information they controlled. Of course, five years ago, most public coverage circled around major banks, based on the Willie Sutton quote about robbing banks "because that's where the money is." At the time, several financial regulators were swinging their "Eye of Sauron" toward the elements of their sector they deemed most vulnerable. As a result, we've seen half a decade of cyber sweeps, recommendations, and requirements through the Security Exchange Commission (SEC) and other financial regulators.

A lot has happened in five years. I've grown from my early experiences at LegalTech, where, as one of three security vendors, I was lost in a sea of document management and sexy e-discovery vendors. The legal community has come under fire, been the victim of a multitude of public attacks, and learned its lessons the hard way. And the second edition of the ABA Cybersecurity Handbook reflects a more seasoned approach to cybersecurity and client obligations. Jill D. Rhodes reprised her role as editor and was joined by Robert S. Litt.

The handbook is organized into four major sections: 1) cybersecurity background information; 2) an overview of legal and ethical obligations; 3) specific considerations of different legal practices; and 4) incident response and cyber insurance. The book is a must-read for attorneys, but also senior level security personnel in law firms, or those officers responsible for risk and compliance oversight. In fact, it provides a deep dive into the National Association of Corporate Directors (NACD) *Director's Handbook on Cyber-Risk Oversight* that frames out the fiduciary

responsibilities of board and executive officers. The reality is that it's not just about protecting your reputation or your client's information. Today, the stakes are much higher and the damage associated with cybercrime is far reaching with a high risk of material damage to the affected business.

The ABA Cybersecurity Handbook contains noticeable depth and exploration of cybersecurity risks, drawing from a plethora of anecdotes, findings, and post-breach outcomes with which to frame the risks facing law firms. The exploration of threats, such as social engineering, ransomware, and business email compromise (BEC) demonstrates that both sophisticated and non-technical attacks continue to plague law firms (as they do across most industries). Data from eSentire's security operations center (SOC) shows two significant trends.

The first trend is that over five years, law firms have improved their cybersecurity hygiene and practices, which has reduced the overall number of successful attacks and even eliminated much of the background radiation type of threats. In fact, in 2017, law firms saw up to 10% less of these attacks compared to businesses in finance, healthcare, energy and others. Unfortunately, law firms saw over 30% more malicious code attacks, which aligns with other industries that have strong cybersecurity practices, such as financial institutions. So, what does this mean? As an industry, the majority of unsophisticated criminals give up and look for easier prey, but that leaves us with the talented criminals who continue to prowl for valuable confidential information.

The handbook also explores how to address these threats and considers the risks associated with the critical technologies that now pervade law firms. The book provides greater depth around regulatory requirements and international legislation and explores when and how counsel should initiate a conversation with the client about cybersecurity (let's hope most are proactive and not reactive, in the event of a breach). More often than not, the client initiates the conversation based on the nature of their business, the sensitivity to reputational or intellectual damage, or presence of a regulator in their market.

Those who have heard me speak on this topic know the client is the new regulator. And for those who haven't, I'm certain you shudder at the words "cybersecurity due diligence." This information forms the basis from which attorneys, administrators, and clients must consider inherent risks, eliminating some, mitigating others, and accepting the risks that cannot be removed. At a minimum, this information serves to establish a level of protocol across the law firm, no matter an individual's role.

The second key trend explored in several chapters of the second edition reveals the specific sensitivity of the varying, yet potentially damaging information controlled in different types of practices. And this is the critical message: No matter your practice, you still have unparalleled access to critical, potentially business altering, client information. Law firms are privy to myriad confidential information that can be used to front run trades, evade prosecution, or perhaps topple governments (at least select politicians).

Last year's attack on Wall Street law firms Cravath, Swaine & Moore LLP and Weil, Gotshal & Manges LLP demonstrated how stolen information, such as FDA filings and press releases, could be used to front run trades. The Paradise Papers represents the next evolution of the Panama Papers. Even tax law information can be monetized or weaponized by (self-proclaimed) ethical hackers. Even an off-the-radar law firm in a tropical paradise could house the type of information that can destabilize a government or ruin the career of elitist politicians and socialites. It's a privilege to be exposed to the fuel that drives our economy, but it's also a responsibility. No one practice is the same. And the specific nature of your firm should be taken

into consideration when developing a risk assessment that will serve as the compass used to map out your cybersecurity programs.

Of course, the type of practice is one element that helps frame a sound cybersecurity practice, but the size of the firm often sets the budgetary tone. A small law firm cannot afford the security technologies and practices adopted by their larger peers. And it's not unreasonable to think that the standards, to which a large law firm is held, are not the same as those that a small firm can manage. There is no one-size-fits-all when it comes to establishing standards of reasonable care. To this end, the second edition offers guidelines for both large law firms and "the little guy." Ransomware doesn't prejudice by size of firm. It just locks files and demands payment. All too often, smaller firms have no back-up mechanisms in place and fall victim to such extortion; whereas larger firms use multi-level back-up services to weather these kinds of attacks. The book contains a resource-right-sized approach with a 12-point checklist that smaller firms can use to build a simplified cybersecurity program.

For larger firms, the recommendations are more strenuous and strike a tone of requirement rather than "nice-to-have" or "try-your-best." The recommendations are aligned to industry best practices and reflect the core tenants of other security frameworks, such as NIST and HIPAA for healthcare firms. This section of the handbook lacks in practice guidelines and establishing "must-haves" compared to more aspirational goals in a cybersecurity program. And like NIST, such a program should start with an analysis of its current state to determine the gaps that need closing to reach the desired state.

This is where related organizations, such as ILTA, could do more to publish these sorts of findings and help build a subjective standard of care. As in "this is what most firms of similar size are doing." The recommendations also include guidelines such as, "firms should log and monitor network access and deploy data loss prevention tools to monitor where data is going and to flag or block unusual file transfers." Such guidelines are high-level and, to some degree, outdated. That is not to say firms should not employ logging or data loss prevention systems, but it ignores the cost and complexity of such systems. And it does not include other systems, such as endpoint protection and real-time detection and response services that are growing in adoption. Nonetheless, this second edition takes many good steps forward in its thoroughness and recommendations. For more details, I would refer to the aforementioned NIST and HIPAA frameworks that provide greater detail.

The second edition of the *ABA Cybersecurity Handbook* is a must read and should have a place on the desks of any attorney and firm's cybersecurity leaders. The book does an excellent job of outlining *what* to do to improve firm and attorney cybersecurity practices. With that said, the one future improvement I would like to see is for the ABA to suggest the *how*. That is, a framework that is tailored to law firms, with specific critical, important, and "nice-to-have" services based on firm size. The point here is not to be prescriptive for sake of control. It's more about setting a collective industry bar (pardon the pun) that establishes a standard of care to which all firms can aspire and better protect their reputation and clients.

*****

Mark Sangster is a cybersecurity evangelist who has spent significant time researching and speaking to peripheral factors influencing the way that legal firms integrate cybersecurity into their day-to-day operations. In addition to Mark's role as VP and industry security strategist with managed cybersecurity services provider eSentire, he also serves as a member of the LegalSec

Council with the International Legal Technology Association (ILTA). He can be reached at mark.sangster@esentire.com.

—❖—

Password-Sharing May Be a Federal Crime under the Muddied Waters of the CFAA

By Shain Khoshbin and Aaron Dilbeck

The Computer Fraud and Abuse Act (CFAA) is a federal statute that provides for not only criminal liability, but also civil liability, when a person accesses a computer "without authorization" or "exceeding authorized access." However, as a result of differing opinions among federal circuit courts, the scope of actionable conduct under the CFAA remains unclear. And due to high-profile cases such as *United States v. Nosal* and *Facebook v. Power Ventures*, the CFAA has recently drawn increased attention from practitioners and scholars alike — often hoping for the Supreme Court to end the lack of clarity under the statute. This has not yet happened. Nevertheless, this attention has led to the issue of when and how can password sharing be subject to criminal (and civil) liability.

The CFAA's Muddy Waters

There has been much debate and consternation over what the phrase "exceed authorized access" in the CFAA means. Numerous articles have addressed this issue and the circuit split concerning this issue. Nonetheless, some of this attention and analysis has been misplaced.

For example, some commentators and practitioners have mistakenly conflated the phrase "without authorization" (which is not defined in the CFAA) with the phrase "exceeds authorized access" (which is defined in the CFAA) — often just referring generically to "authorization." Further muddying the waters, some courts have interpreted the defined term "exceeds authorized access" narrowly (to avoid making an act commonly subject to civil liability into a criminal act), and other courts have interpreted it broadly (to make everyone liable for his/her cybermisdeeds). Indeed, that phrase has led to "a subtle and fraught inquiry" (*Facebook Resp. to Pet. for Cert.* p. 12) into whether "exceeds authorized access" includes using a work computer for non-work purposes, violating a terms of use agreement, and accessing information in one part of a network for which permission was not expressly given. Unfortunately, the Supreme Court has yet to uniformly define the CFAA's phrase "exceed authorized access."

Password Sharing in the CFAA's Muddied Waters

This lack of uniformity in the law has become a subject of growing concern, including concern over whether the statute transforms mundane and nonmalicious acts — those that may otherwise be a civil issue—into a criminal matter. For example, in *United States v. Nosal* (9th Cir. 2012) (*Nosal I*), a former employee of a company conspired with current employees of that company to use their passwords to access and download files from the company's database to start a competing business. In basically ruling that violating terms of use does not constitute violating the CFAA, the *en banc* panel stated: "If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions — which may well include everyone who uses a computer — we would expect it to use language better suited to that purpose."

Then later in *United States v. Nosal* (9th Cir. 2016) (*Nosal II*), the U.S. Court of Appeals for the Ninth Circuit held that those former employees violated the CFAA because, after their former employer revoked their access to its computers, they used a current secretary's password to

access the computer. In sum and substance, that revocation was all that mattered for the majority's opinion as it concerned violation of the CFAA. Significantly, in his dissenting opinion in *Nosal II*, Judge Reinhardt noted that — under the majority's opinion — one spouse may be in violation of the CFAA for using the other spouse's password (with permission) to pay a bill on their bank's website. To further illustrate his concern, Judge Reinhardt noted that the majority's interpretation of the CFAA may turn a parent's checking his child's email account into a federal crime.

This issue was recently highlighted in *Facebook v. Power Ventures* (9th 2016). In that case, Power Ventures, a social networking company, received permission from Facebook account holders to access their accounts and aggregate the social media information in one place. While the account holders desired such a service that aggregated their information, Facebook did not approve and sent Power Ventures a cease and desist letter. When Power Ventures disregarded Facebook's cease and desist letter, Facebook sued it for violating the CFAA. And although Power Ventures had the account holders' permission to access their accounts, the Ninth Circuit affirmed the lower court's holding that Power Ventures was liable for accessing Facebook's computers "without authorization."

When all is said and done, it may be that the courts have lost their way with regard to the purpose and scope of the CFAA. Or, at a minimum, both the courts and the legislature have not been able to keep up with the velocity of changes in technology as it concerns the CFAA. Originally titled the Counterfeit Access Device and Computer Fraud and Abuse Act, the CFAA was enacted in 1984 to address the theft of classified information from government computers. In fact, the CFAA was exclusively a criminal law until it was amended in 1994 to also provide for civil liability. The most recent amendment was introduced in May 2008, less than a year after the release of the first iPhone and before a single Android device was sold.

The Jersey in the Locker

Perhaps part of the confusion in the law arises from the fact that computers have become so much more than a machine that a person uses to process and keep his/her own information. In fact, in today's day and age, and increasingly so, "computers" often contain someone else's information. Herein may lie some insight into the issue with the CFAA and password sharing. Consider a computer and the data in that computer as a locker and a jersey in that locker. Computers can be password protected and lockers can be pad-locked. Also, data can be stolen without harming the computer like a jersey can be stolen without damaging the locker. *Power Ventures* essentially held that the locker owner has a CFAA cause of action against someone who takes the jersey in the locker, even though the jersey's owner gave that someone the pad-lock combination and permission to take the jersey. Indeed, that person who took the jersey with permission of its owner could be held criminally liable for this seemingly innocent act. Yet, *Nosal I* essentially held that the locker owner did not have a CFAA cause of action against someone who wrongfully takes the jersey, which belongs to the locker owner, because the locker owner at one point gave the pad-lock combination to that someone to use the locker. Then, *Nosal II* essentially held that the locker owner had a CFAA cause of action against someone who takes the jersey, which belongs to the locker's owner, even though that someone received the pad-lock combination from a person authorized by the locker owner to use the locker.

Insights Into the CFAA Arising from Jersey-in-the-Locker Comparison

In sum, while the owner of the information and the computer where it is stored are often the same, the two different properties can easily have different owners in today's age of the Internet, social media, and cloud computing. As it concerns "password sharing" (where there is no

damage to the computer system itself), perhaps one method to resolve inconsistencies in the interpretation and application of the CFAA is to start focusing the analysis on who owns the information in the computer for which the password is being used. It is noteworthy that the CFAA was originally enacted to protect government information contained in government computers from cybercriminals. Now, however, a social media company has been held liable under the CFAA because it accessed a Facebook account holder's posts, after receiving permission from that account holder to do so.

The judiciary, or preferably Congress, needs to address the CFAA's lingering issues, including exactly what and whom the CFAA was *meant* to protect. Indeed, in addition to conflicting opinions over the meaning of "exceeds authorized access," courts also disagree about what constitutes an actionable "loss" under the CFAA. In the meantime, however, the CFAA remains a useful tool to businesses as a part of their crisis management plan(s) for data breaches, and to seek justice from those who improperly access electronic assets. Because of the ongoing debates and uncertainty regarding the scope of the CFAA, businesses need to plan ahead to realize the statute's value. For example:

- If possible in the given business model, companies should ensure that data they wish to protect is password protected (and even separately password protect different databases in the same network) because — in the first instance — the issue of authorization may turn on whether the information is adequately password protected or publically available. *See, HiQ v. LinkedIn, (N.D. Cal. 2017)* (now on appeal);
- Carefully issue passwords (with regular updates), specifically limit authorization to those password-protected databases, and delineate the purpose of such access; and
- Effectuate policies, procedures, terms and conditions and/or user agreements that delineate such protections, including the prohibition of password sharing and automatic termination of rights of access/authorization upon certain defined events.

*****

Shain Khoshbin *is a partner at Munck Wilson Mandala in the complex litigation/dispute resolution group.* **Aaron Dilbeck** *is an associate at the firm, practicing in the complex litigation/dispute resolution group. His practice is focused on intellectual property disputes and commercial litigation.*

—❖—

Cybersecurity Spending at Law Firms, Legal Departments Is Predicted to Increase in 2018

By Ed Silverstein

As law firms and legal departments finalize their 2018 budgets, many lawyers in both the United States and Canada plan to increase cybersecurity spending.

A recent survey from Robert Half Legal found that 41% of U.S. lawyers said that their law firm or company plans to increase spending on cybersecurity-related tools and services in the next 12 months.

"One of the key reasons that legal organizations are increasing spending is that legal organizations recognize they are a particular target for cyberattacks due to the high volume of

sensitive information they maintain," Jamy Sullivan, executive director of Robert Half Legal, told our ALM sibling *Legaltech News*.
"One can consider the significant volume of valuable client data they hold for companies and organizations of all sizes — intellectual property agreements, contracts, customer, supplier and financial information, research on potential corporate mergers, and evidence in potentially high-stakes litigation cases," Sullivan added. "If this valuable and confidential information falls into the wrong hands, it could prove costly to a law firm as well as its clients, and also cause irreparable damage to brand and reputation."
Therefore, Sullivan said that many organizations are placing a priority on enhancing data privacy policies. And given the "serious legal and ethics violations" that a law firm can face when losing "a client's confidential data to an attack," a proactive cybersecurity strategy is "a commonsense strategy," she noted.
What's more, heightened media focus on breaches and security threats is raising awareness of the importance of security protection. In response, Sullivan said that clients are "applying more pressure onto their legal counsel to safeguard their information." These factors are leading law firms to shift greater attention and resources to address information security and escalating cyberthreat matters.
"Legal counsel have become integral to an organization's ability to develop and implement cybersecurity defenses that meet regulatory expectations and legal requirements and mitigate legal risks — as well as respond and manage legal issues when a security breach takes place," Sullivan said. "Law firms and companies are making cybersecurity an important area of focus for their legal and IT [information technology] teams."
In a related Robert Half survey, 35% of Canadian lawyers said that their law firm or company plans to spend more on cybersecurity-related tools and services in the next 12 months.
Gartner has released its own enterprise study that predicts global spending on cybersecurity will increase to $96.3 billion in 2018. That is an increase of 8% from 2017. Moreover, Gartner said that security testing, information technology outsourcing, and security information and event management (SIEM) are expected to be "among the fastest-growing security subsegments driving growth in the infrastructure protection and security services segments."

*****
Ed Silverstein writes for *Legaltech News*, an ALM sibling of *Cybersecurity Law & Strategy*.

—❖—

Legal Tech
Peril in Paper: *EEOC v. GMRI* and the Digital Divide in e-Discovery Sanctions

By David Horrigan

There was a time not so long ago when the term "e-discovery" didn't exist. It was known simply by its legal name, discovery. We're now entering an era where some observers feel the term will fade into history, returning us back to simply calling it discovery.
Why?
Because — the theory goes — we're now at a point where just about all evidence is electronic, making the insertion of the "e" redundant.

However, the recent federal district court decision in Florida, *EEOC v. GMRI, Inc.*, No. 15-20561 (S.D. Fla. Nov. 1, 2017), not only illustrates that we shouldn't be too quick to ignore paper discovery, it serves as an excellent tutorial on the different legal standards for paper and electronic data. In addition, the case illustrates the information governance and data security considerations when responding to discovery with both digital and paper components.

At Their Peak

Based in Orlando, FL, Seasons 52 is a chain of 41 restaurants with locations across the nation from New York to California. Billing itself as a "celebration of what's good now," Seasons 52 markets itself to patrons as restaurants with a "casually sophisticated setting" and seasonably inspired menus featuring ingredients at their peak of freshness with features such as open-fire grilling and an ever-changing selection of global wines.

Operated by GMRI Inc., formerly General Mills Restaurants Inc., the chain is part of Darden Restaurants, a 1,500-restaurant operation including national brands such as The Capital Grille, LongHorn Steakhouse and Olive Garden.

Seasons 52 may market itself as celebrating what's good now with ingredients at their peak, but if a complaint from the U.S. Equal Opportunity Employment Commission (EEOC) is to be believed, something Seasons 52 didn't think was good now and at their peak were older workers.

Older Applicants

Anthony Scornavacca and Hugo Alfaro applied unsuccessfully for server positions in 2010 at Seasons 52's Coral Gables, FL, location. The two later filed independent discrimination complaints against Seasons 52 under the federal Age Discrimination in Employment Act (ADEA). Neither Scornavacca nor Alfaro asserted class-wide allegations or theories that extended beyond their own individual circumstances.

The EEOC notified Seasons 52 of the charges and explained the Commission's record-keeping requirements.

There was a dispute between the EEOC and Seasons 52 about whether Seasons 52 ever received an Aug. 31, 2011 EEOC letter notifying Seasons 52 that it was expanding the investigation to include the chain's hiring practices throughout the nation. But, on Jan. 10, 2012, a Seasons 52 paralegal wrote a letter to the EEOC denying that Seasons 52 maintained a nationwide policy not to hire people over the age of 40.

Paper Policies and Productions

Established in 2010, Seasons 52's own document retention polices required employment applications of unsuccessful applicants be retained a minimum of three years and the applications of those hired to be saved for at least six years. The policy also provided for legal holds on email to be initiated by counsel and implemented by IT staff.

In the EEOC investigation, the Commission requested employment applications to analyze Seasons 52's hiring of older workers. The EEOC alleged the company's collection and production procedures were somewhat lacking.

For locations other than Coral Gables, rather than issue a legal hold, a Seasons 52 "litigation team" merely asked managers to send paper applications to a central office to be scanned. The productions were less than comprehensive, however.

According to restaurant managers, the Tampa location had received approximately 1,800 applications, but it produced only 205. The King of Prussia location produced only 325 of about 1,000; Costa Mesa produced only 322 of its 1,000; Jacksonville produced 126 of 1,000; and the Kansas City restaurant produced only eight applications out of an unknown number.

The Coral Gables restaurant illustrated a disparity between electronic and paper data. Electronic data at that location indicated Seasons 52 actually favored older workers, but paper data showed a statistically significant failure to hire older workers.

In addition to paper applications, Seasons 52 had so-called interview booklets where managers took notes and scored applicants. Some locations used electronic versions while others still used paper. Because Seasons 52 produced such a small percentages of the paper booklets, the EEOC alleged Seasons 52 had destroyed many of them despite its legal obligation to retain and produce them.

Electronic Preservation

From 2010 to 2014, Seasons 52's production of electronically stored information (ESI) wasn't much better. Its NearPoint Mimosa archiving system automatically deleted email after 90 days unless a legal hold was issued. In February 2014, Seasons 52 switched to a ProofPoint archiving system with an automatic thee-year retention for all email.

To complicate matters, although Seasons 52 issued a legal hold for Coral Gables in 2010, it didn't issue a legal hold for the rest of the chain until 2015. In addition, it failed to preserve any hard drives.

Despite the data not produced, Seasons 52 argued it conducted comprehensive e-discovery, collecting all email and workstation documents from over 100 custodians while responding to ever-increasing EEOC demands.

The company noted it collected over 2,300 gigabytes of data, totaling more than 5,500,000 documents. It then applied more than 1,500 negotiated search terms to the collected data. The searches returned approximately 620,000 documents for review and cost hundreds of thousands of dollars to complete. Seasons 52 then produced about 31,000 ESI records, totaling more than 110,000 pages.

Defining and Sanctioning Spoliation

When analyzing potential legal liability for the allegedly destroyed evidence, the court in the Seasons 52 litigation noted courts have not been consistent in defining, "spoliation," the destruction or alteration of evidence. The question is whether spoliation by its definition is intentional destruction.

Because the 11th Circuit in *Green Leaf Nursery v. E.I. DuPont de Nemours & Co.*, 341 F.3d 1292 (11th Cir. 2003), did not require spoliation to be intentional, the Seasons 52 court didn't require it either.

Claiming Seasons 52 destroyed evidence it knew was responsive to EEOC requests, the Commission sought an adverse inference instruction to jurors as a sanction for the spoliation. Citing *Bashir v. Amtrak*, 119 F.3d 929, 931 (11th Cir. 1997), the court held an adverse inference instruction is appropriate only when there is evidence of bad faith. Thus, citing *Preferred Care Partners Holding Corp. v. Humana, Inc.*, 08-20424-CIV (S.D. Fla. Apr. 9, 2009), the court held even grossly negligent conduct did not warrant an adverse inference instruction.

The adverse inference instruction the EEOC sought on the paper documents was an instruction to jurors that the missing paper documents at some locations would have shown more significant under-hiring of older workers than indicated in the electronic data. For other locations, the EEOC sought an instruction that the missing data would have provided anecdotal testimony of age discrimination.

For the electronic documents, the EEOC sought an instruction that the missing emails would have indicated a preference for younger workers.

The court noted that the adverse inference sanctions the EEOC requested required a showing of bad faith, but that lesser sanctions — such as limiting or excluding evidence or allowing a jury to consider evidence of spoliation — required no such showing.

Paper v. Electronic

The court noted there were different legal standards for sanctions with paper and electronic data. It could use its inherent powers to sanction paper spoliation, while sanctions for spoliation of ESI were based on Fed. R. Civ. P. 37, which — for the most severe sanctions, including an adverse inference instruction — required a showing of an "intent to deprive."

In the end, citing *Managed Care Solutions, Inc. v. Essent Healthcare, Inc.*, 736 F. Supp. 2d 1317 (S.D. Fla. 2010), the court declined to issue the most severe sanctions for the paper documents because it believed the evidence was not crucial for the EEOC to make its case, noting an EEOC expert could analyze the employment information without the missing information.

Thus, on the paper documents, the court allowed the parties to "present competing facts and theories to the jury."

The court said Seasons 52 would have to "confront thorny and awkward evidence" about EEOC theories on the company's failure to timely and comprehensively respond to notices the case had expanded. On the other hand, the court said the EEOC could have been "clearer in articulating its view" that the case had expanded to a national investigation.

On the ESI, relying on Fed. R. Civ. P 37(e)(2), the court permitted the EEOC to argue to the jury that it may reach an adverse inference about missing ESI if (but only if) it concludes that Seasons 52 acted "with the intent to deprive" the EEOC of the ESI's use in this lawsuit. The court said the EEOC was permitted to establish this theory concerning ESI — not the paper applications and interview booklets — without also obtaining a finding of prejudice to the EEOC.

Why Seasons 52 Matters

The EEOC investigation and litigation over Seasons 52's hiring practices provides a textbook example of the perils of paper and digital preservation — as well as the different legal standards for paper and digital data.

Reasonable Anticipation of Litigation

Although "reasonable anticipation of litigation" is a well-known standard for when data preservation must begin, it isn't particularly helpful here. Litigation didn't commence until 2015, but Seasons 52 was subject to regulatory preservation requirements years before. Although the parties disagree on whether the Aug. 31, 2011, EEOC letter was sent or received, by 2012, an investigation required preservation — whether or not litigation ever ensued.

Self-Collection of Data

This is rarely a good idea for litigation or investigations, and it wasn't a good idea here. Because managers merely collected paper applications and sent them to be scanned, it leaves open the question of why such a small percentage of the applications were produced. Were they lost in transit? Did they ever exist? Employment applications, by their very nature, are full of personally identifiable information (PII). From a data security standpoint, self-collection of this type of information is fraught with peril.

Paper v. ESI — Retention Schedules

Physical factors may degrade, displace, or destroy paper documents, but automatic deletion schedules for email and other ESI can put organizations in legal jeopardy. In the Seasons 52 litigation, the company's initial 90-day automatic deletion schedule for email put the company in non-compliance with both EEOC polices and the company's own retention policy. In addition,

with its paper application retention standards of three to six years, the discrepancy between paper and ESI periods helped create havoc.

Paper v. ESI — Legal Standards

The case also illustrates that, as odd as it seems, the legal standards for paper and ESI differ. Much has been made of the 2015 e-discovery amendments to the Federal Rules of Civil Procedure and the changes to Rule 37's sanctions provisions with its "intent to deprive" standard for the most severe sanctions. An important difference in the Seasons 52 litigation was that the EEOC's attempts for sanctions on the paper documents were derailed somewhat by what the court relieved as a lack of prejudice. Although prejudice may be assumed where intent to deprive exists, the EEOC did not have to demonstrate it for the ESI.

Conclusion

Cybersecurity professionals and legal teams have been trained to focus on ESI. It's not surprising. Most data are now electronic, and the systems IT and legal teams use are almost exclusively electronic. However, *EEOC v. GMRI* shows paper can be vital to a litigations and investigations in 2017. Seasons 52 spent hundreds of thousands of dollars to collect millions of documents, but it still faced the prospect of sanctions in a paper-digital divide.

*****

David Horrigan is e-discovery counsel and legal content director at Relativity. An attorney, industry analyst, and award-winning journalist, he served formerly as analyst and counsel at 451 Research and reporter and assistant editor at *The National Law Journal*.

To order this newsletter, call:
800-756-8993

On the Web at:
http://www.lawjournalnewsletters.com/cybersecurity-law-and-strategy

Editorial email: ssalkin@alm.com
Circulation email: mailto:customer care@alm.com
Reprints: www.almreprints.com

Published Monthly By:
Law Journal Newsletters
1617 JFK Blvd, Suite 1750, Philadelphia, PA 19103