OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVI NUMBER I
JANUARY 2019
www.mnbar.org

Bench&Bar OF MINNESOTA

Minnesota's Public School System Goes on Trial

Cruz-Guzman **presses the question of what constitutes an adequate public education**

Uniformity in Trust and Estate Law

A Storm on the Farm

Fair Trials in the Age of Facebook

Plus 2019 Buyers' Guide

"Papers and effects" in a digital age

In 1761, Boston patriot James Otis argued against England's use of its "writs of assistance." Such writs, widely used in colonial times, permitted English officials to enter a Crown subject's private home or office—at will, and without regulation. These warrantless searches, also called "general searches," were used to investigate purported crimes against the Crown.

Otis argued against these writs, saying:

> Now, one of the most essential branches of English liberty is the freedom of one's house. A man's house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle. This writ, if it should be declared legal, would totally annihilate this privilege. Custom-house officers may enter our houses when they please; we are commanded to permit their entry. Their menial servants may enter, may break locks, bars, and everything in their way; and whether they breach through malice or revenge, no man, no court can inquire. Bare suspicion without oath is sufficient.[1]

After the Revolution, the founders prohibited these searches by enacting the Constitution's 4th Amendment. The Amendment forbids unreasonable searches and seizures, and requires that, henceforth, in order to search the government must have a warrant, issued by an independent magistrate, and upon proper cause. A valid 4th Amendment warrant must specify premises, persons, and define the evidence being sought.

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 trials. He is a member of the MN Lawyers Professional Responsibility Board.

And in executing the warrant, law enforcement is limited to seeking and seizing evidence actually related to the crime under investigation. This relationship between the crime being investigated and the search's extent sometimes leads to the aphorism that, "if you are looking for stolen televisions, you cannot look in sugar bowls."

There is, however, a corollary: While an investigator may only search for evidence related to a specific crime, the investigator need not be blind to evidence of other crimes in "plain view." So, while warrants must restrict the scope of the search, further investigations can be initiated if evidence of other crimes is readily observable.

A constitutional warrant, thus, protects citizens from general searches and unregulated intrusions into the citizen's person and property.

Citizens are protected against the "bare suspicions" against which James Otis argued. A specific warrant is critically important in protecting personal freedom.

But how do these principles translate into our increasingly digitalized world? Is a cell phone or a personal computer an object "in plain view?" The question is especially urgent now, when such devices may contain a vast array of extremely personal material about its owner, as well as evidence of a particular crime or material highly relevant to a legitimate investigation.

By way of a simple example, assume a person's cell phone or laptop computer holds a "notes" file showing drug debts owed, or drug proceeds taken. And assume an investigator obtains a valid warrant for those notes. Is that investigator, when analyzing that phone or computer, prohibited from looking into photo files that might reveal the owner trafficked in child pornography? The law is only beginning to grapple with these kinds of questions.

Part of the law's grappling has been felt in terms of revised admissibility standards. New amendments to Federal Rule of Evidence 902 address digital records such as those collected and preserved from devices, including emails. These additions make digital records submitted as evidence self-authenticating, meaning no additional evidence is required for admission in court:

> (13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

(14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).[2]

Even with these rules now in place, it still remains to be seen how the courts will apply them. It is clear that movements toward standardizing data collection and authentication are being made, and that adherence to proper procedures regarding digital evidence is increasingly recognized. Given the huge amounts of data stored on digital devices, admissibility issues are particularly important in examining 4th Amendment considerations. In addition to the need to stay within the limits set forth in a warrant, evidence admissibility requirements also protect a person's "papers and effects" and regulate what is allowed.

It is most unlikely that the 4th Amendment's drafters contemplated a single device that might contain records of personal communications, medical diagnoses and treatments, banking and financial transactions, family matters (remember, photography came far after the Constitution's drafting), and investment holdings, all in the palm of a person's hand.

The authors of this article suggest that the courts need to refine and redefine the 4th Amendment's protection of "papers and effects" as it applies to executing a search warrant of electronic data-storing devices. If an investigator may not look into a sugar bowl to find evidence of stolen televisions, it seems unreasonable to permit the same investigator to indiscriminately rummage through a citizen's smart phone or personal computer. ▲

Co-author Hon. JAMES M. ROSENBAUM (Ret.) served 25 years on the federal bench as a United States District Court Judge for the District of Minnesota and served as chief judge of the district. For the four years prior, he served as Minnesota's United States Attorney.

Notes

[1] *http://www.constitution.org/bor/otis_against_writs.htm*

[2] *https://www.rulesofevidence.org/article-ix/rule-902/*

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVI NUMBER V
MAY/JUNE 2019
www.mnbar.org

Bench&Bar OF MINNESOTA

The Guns Aren't Illegal. But Sometimes the Owners Are.

Understanding Minnesota's private-transfer exception suggests the best path to reducing gun violence

Your smartphone and the 5th Amendment

Lessor beware: Tenant trademark infringement

Lessons learned from the Lunds *shareholder litigation*

"Papers and effects" in a digital age, pt II

Modern information technologies are testing the United States Constitution's protection against government intrusion. In our article "'Papers and effects' in a digital age," published here in January 2019, we looked at the impact of smartphones and the challenges they pose for search warrants and government investigators. We concluded that as our technological landscape rapidly expands and evolves, so too do courts need to adjust to maintain the degree of privacy afforded by the 4th Amendment.

Our digital age has forced courts to reevaluate the balance between privacy concerns and the government's legitimate interests when digital devices are seized during investigations. Just as the founders sought to bar Britain's writs of assistance and the Crown's ability to indiscriminately search private homes or offices, we again face the need to establish acceptable boundaries for warrant-authorized searches. Modern digital telephones and electronic devices regularly contain vast amounts of their owners' personal information. This new reality means that government investigators must have carefully defined limits when they seek to review these items or locate electronically stored evidence. Courts are responding to these concerns.

Case in point: *Riley v. California*

In 2014, the United States Supreme Court considered the case *Riley v. California* (573 U.S. __ (2014)). Mr. Riley had been arrested for a traffic violation. His cellphone was seized incident to the arrest. Police officers, without a warrant, examined information stored on the phone; they discovered photos and videos that suggested gang involvement. This stored information led to Riley's being charged in connection with a shooting that occurred weeks earlier. He challenged the digital search, raising the question of what investigators are allowed to search on digital evidence. The lower courts found that the digital search incident to Riley's arrest allowed the evidence.

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

The Supreme Court reversed. It recognized that, historically, officers were permitted to examine objects seized incident to a lawful arrest. But in 2014, the Supreme Court held that a modern digital phone was not just another object; its ability to store vast amounts of data called for a deeper consideration of the effect of its seizure. In today's technological landscape, the average person stores a huge amount of data about their daily lives. This reality is unprecedented; even in the rare event that an officer found a personal diary on a person incident to an arrest, that diary would contain a limited amount of information. The Court set aside issues of officer safety or evidence destruction, neither of which was materially implicated in the seizure of a cellphone. Instead the Court found that, in considering digital devices, "a search of digital information on a cellphone… implicates substantially greater individual privacy interests than a brief physical search[.]"

> The law is properly recognizing that our digital world requires a new level of warrant specificity.

The Court further held that the threat of evidence destruction, either by remote wiping or encryption, was not substantial enough to merit a warrantless search. Many investigators argue that warrants hold up investigations, making it difficult if not impossible to properly examine digital evidence. However, investigators can take immediate action to secure digital devices for future analysis, including turning off the devices and using Faraday bags, which help to protect against the threat of remote tampering.

A unique information source

Even the most basic smartphone has significant storage capacity and often holds information spanning the course of several years. Cloud computing and the existence of data stored on remote servers that can be easily accessed via smartphones further complicates the search process, since the accessible data technically extends beyond the physical confines of the phone itself.

In spite of these issues, the Court emphasized that "the Court's holding is not that the information on a cellphone is immune from search; it is that a warrant is generally required before a search[.]" The nature of our digital world justifies the need for warrant specificity.

The law is properly recognizing that our digital world requires a new level of warrant specificity. For the majority of Americans, these devices contain private details about almost every, if not every, aspect of our lives. The fact that technology now enables an individual to carry such information in his hand does not make the information any less worthy of the protection for which the founders fought. Our answer to the question of what police must do before searching a cellphone seized incident to an arrest is accordingly simple—specify what you are searching for and get a warrant.

The Supreme Court's emphasis on the need for a warrant should not unduly impede the competent investigator. Any issues posed by needing to wait to obtain a warrant can be readily mitigated. Indeed, the same kinds of electronic access can be used to obtain warrants electronically. Many states and federal procedures provide for electronic warrant application and authorization. This is an area where the law is fast developing, as the courts apply timeless principles to evolving situations. As illustrated by the *Riley* case, digital devices have vastly expanded the scope of information which may be available in seized objects. The law is beginning to consider these new factors. ▲

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXV NUMBER III
MARCH 2018
www.mnbar.org

Bench&Bar OF MINNESOTA

#MeToo IN THE LAW FIRM

Lessons for lawyers from the post-Weinstein reckoning

#MeToo as a moment opportunity

How to change firm culture

Trump Year One: A conversation with immigration lawyers

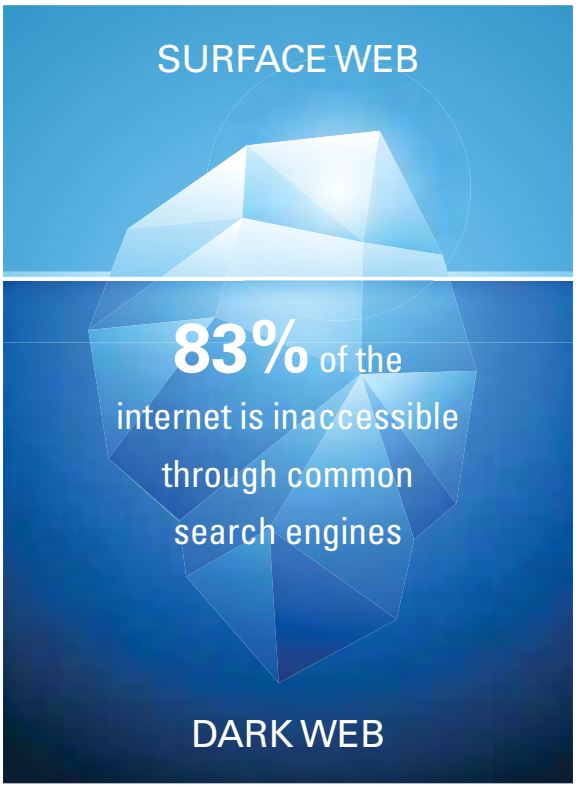
Beyond the travel ban: Headaches for employers

Stephen Allwine:

When crime tries to cover its digital tracks

In late 2016, I was approached by the Washington County (MN) Attorney's Office to conduct forensic analysis on a number of devices in a homicide investigation. It soon became clear that the case would be one of the most interesting of my career, involving murder-for-hire, religious convictions, insurance money, infidelity, and a distinctly modern element—the Dark Web—that combined to make for one of the most tragic and complex cases I've encountered.

The Dark Web, a broad term used to describe the 83 percent of the internet inaccessible through common search engines like Google or Bing, is where many people go to find illegal drugs, child pornography, stolen credit card numbers, and hacking services (though not every service and product available in this online marketplace is illegal). Enter defendant Stephen Allwine: After his attempts to hire a hitman on the Dark Web failed, Allwine murdered his wife in their Cottage Grove home and staged it as a suicide. In January 2018, Allwine was sentenced to life in prison; forensic analysis played a critical role in fleshing out the narrative details that helped the jury make their decision.



MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 trials. He is a member of the MN Lawyers Professional Responsibility Board.

In 2015, Steve Allwine began exploring a website known for neither its upstanding moral quality nor its cybersecurity strength—Ashley Madison. Through this cheating website, Steve began experimenting with extramarital affairs and the underbelly of the internet. Analysis of Allwine's devices revealed communications with at least two women through the site; their conversations illustrated Allwine's dissatisfaction with his marriage and his desire to become involved with other women, unhindered.

Exploring the Dark Web

While Ashley Madison itself is not part of the Dark Web, I would consider it to be a kind of gateway to the darker aspects of internet usage. It wasn't long after his first few Ashley Madison-initiated affairs that the Dark Web became a prominent part of Steve Allwine's browsing.

Jurors learned that Allwine first discovered Ashley Madison as a marriage counselor for couples in his church. Though Allwine ultimately initiated affairs through this site—many users who sign up for Ashley Madison and similar cheating sites don't actually end up having affairs—he still did not regard divorce as an option. Constrained by the marital requirements of his church, Allwine took a dive into the Dark Web to search for other solutions to his predicament. It wasn't long before Allwine discovered Besa Mafia, a Dark Web group claiming to provide anonymous hitman services.

Besa Mafia was a Dark Web vendor that advertised themselves with the slogan "Hire a killer or a hacker." The enterprise was later revealed to be a scam, but Allwine—using the pseudonym "dogdaygod"—communicated extensively with Besa Mafia, communications which were subsequently released to the internet. These communications included multiple references to Amy Allwine and included her home address, phone number, physical description, and a photograph. One particularly thorough attempt to organize the hit once and for all involved Allwine providing particular location information, a current picture, and a description of her vehicle. Of particular note was the photo shared, which was subsequently discovered in a folder on one of Allwine's devices. But the hit he sought to arrange never occurred, and Allwine would later report his lost thousands of dollars to the police.

While Allwine clearly endeavored to remain invisible on the Internet, a key piece of evidence unequivocally tied him to a Bitcoin payment made to Besa Mafia for the murder of Amy Allwine: a unique, 34-digit alpha-numeric Bitcoin wallet address typed out in his iPhone's Notes app that had been deleted. This Bitcoin address matched the one used by "dogdaygod" to make a payment to Besa Mafia.

Though Bitcoin has become increasingly popular in recent months even among non-Dark Web users, it remains the preferred currency for Dark Web exchanges. The address found in Steve Allwine's deleted note proved to be critical to the case. As Washington County prosecutor Fred Fink explained later, "It was absolutely vital for the State to prove that 'dogdaygod' was, in fact, Stephen Allwine. With that connection made, we were able to show intent to kill and premeditation."

A pattern of deception

My analysis of Steve Allwine's devices also reveal a steady pattern of anonymizing service use, disposable account creation, and a desire to conceal his identity from law enforcement. My office was provided with a staggering 66 devices—a huge number in comparison to the typical homicide case. Allwine used multiple devices to further obscure his online activity. On his Reddit account, also using the pseudonym "dogdaygod," Allwine frequently researched questions pertaining to safe use of the Dark Web, the likelihood of law enforcement presence on the Dark Web, how to use disposable computers, and how to remain anonymous on the Internet. To access the Dark Web, Allwine used virtual private network services and the TOR network. These services act as portals to the Dark Web and encrypt accessed information by relaying it through a series of other networks. Incredibly, Allwine also used disposable email accounts to report evidence of his stolen Bitcoin to police after the hit did not materialize. He even created a fictitious person to frame for the stolen Bitcoin.

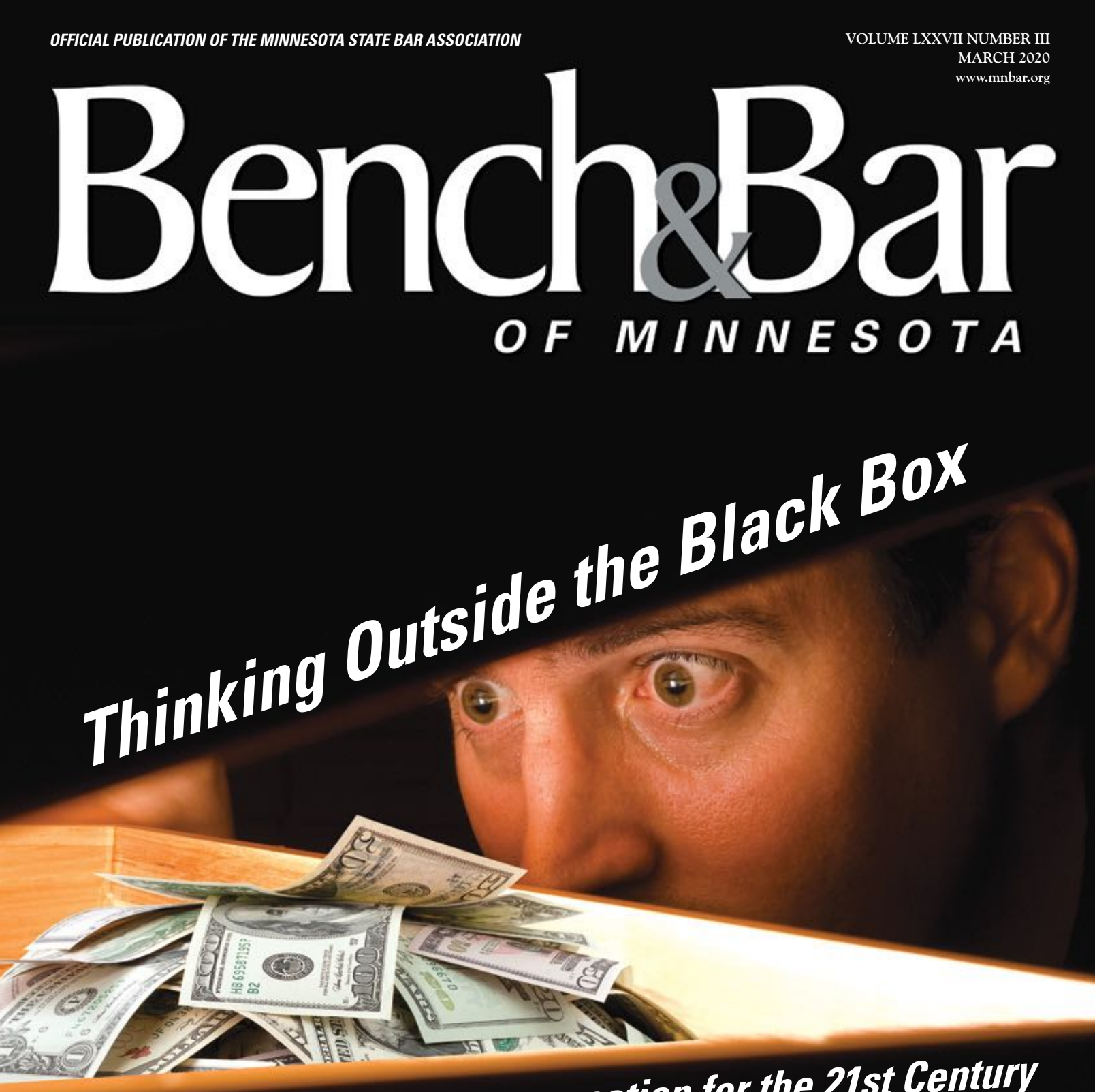
Allwine's digital narrative also revealed a browsing history consistent with his intention to murder Amy and his desire to frame fictitious parties. On more than one occasion, Allwine reviewed his and Amy's insurance policies as well as real estate and future home construction possibilities. In an effort to blame an unidentified third party, Allwine sent his wife a threatening email using an anonymous email service—after he had used doxxing (the process by which personal information is bought and sold on the Internet, often with malicious intent) to uncover information about Amy's family to personalize his email and make it appear as if it was sent by a business rival.

Ultimately, forensic analysis shed light on the actual truth of what occurred, which pointed solely to Stephen Allwine as the guilty party. This case incorporates some of the most complicated aspects of digital evidence. It was complex in part because Allwine had done everything in his power to conceal his activity, remain anonymous, and hide as much as possible about his intent. Digital forensic analysis revealed critical details that filled in gaps in the physical evidence—gaps that may have inspired doubt in the jury and led to a different verdict. As Washington County attorney Pete Orput described the role of digital evidence in this case, "Mark's forensic work and testimony about it to a jury made my murder case seem simple and overwhelming, and without this work the case would have been a horse race." ▲

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVII NUMBER III
MARCH 2020
www.mnbar.org

Bench&Bar OF MINNESOTA



Thinking Outside the Black Box

Reimagining attorney compensation for the 21st Century

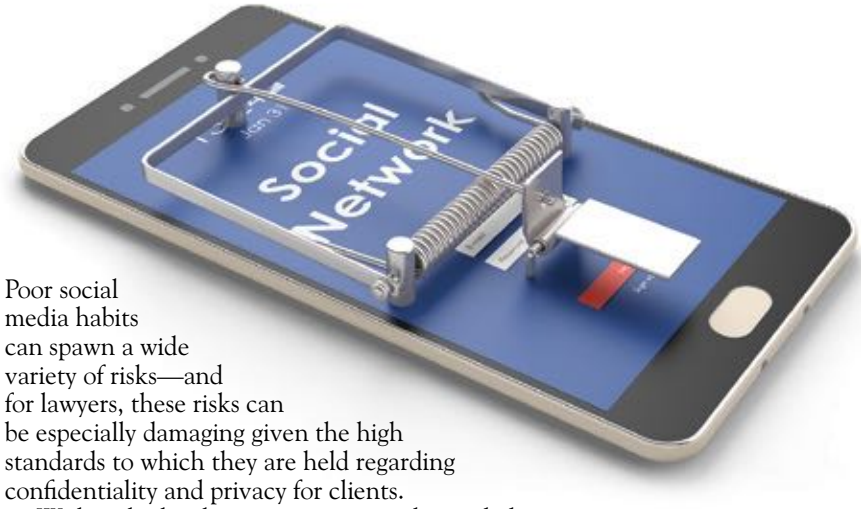
Doxxing made easy: social media

In a recent article, I wrote about doxxing and the potentially unsolvable problems associated with trying to remove all of one's personal information from the worldwide web. In the digital space we live in, where instant communication and the ability to share information within seconds is an ingrained reality, controlling our personal data online is difficult if not impossible. Even if someone were to go through the trouble of carefully combing through 50 sites' (often confusing) opt-out pages and removing their information, there is no guarantee that another reseller website won't pop up the next day with the same information—or that those 50 websites won't simply repopulate within a few months' time. Though we often forget—or deliberately ignore—the fact, anonymity on the internet simply does not exist. But perhaps more troubling is that anonymity in our "real" lives is greatly diminished as well as a result of what can be found online.

We do have a measure of control in one of the digital realms of greatest risk—our own social media accounts. A simple adage comes to mind: Think before you post. It's often easier said than done. After all, some of our wittiest commentaries or observations beg to be shared quickly. Even though most people would likely admit to their lack of anonymity in the social media space, it is also true that many people post and forget. Or they believe that their social media presence is entirely distinct from their professional lives. Many job candidates are horrified to learn that their Facebook posts are up for review just as much as their painstakingly polished resumes.

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

Those seeking positions with security clearances are even more at risk of having their social media presence factor into their assessment as job candidates. For up and coming generations that have used social media for the majority of their lives, it's often a tough truth to accept that once something is "out there," it's never truly gone and might affect their real lives.



Poor social media habits can spawn a wide variety of risks—and for lawyers, these risks can be especially damaging given the high standards to which they are held regarding confidentiality and privacy for clients.

Within the legal community, a poorly worded post or an inappropriate picture can cost a firm in more than one way. A damaged reputation can cost a firm clients, and oversharing online can facilitate cyberattacks, as I have discussed in a previous article, "Social media and managing reputational risk." Doxxing, the process by which personal information is gathered online—often with the intent to maliciously disseminate it—can start with a cybercriminal reviewing a target's social media pages. A seemingly innocent post about going on vacation can be invaluable in personalizing a phishing attack or strengthening a social engineering scheme. Anything shared online can potentially be used to harm a firm financially, operationally, or reputationally. I frequently advise people to not post anything online that they wouldn't want their moms to read. It might be better to also advise people not to post anything that they wouldn't want a cybercriminal to read.

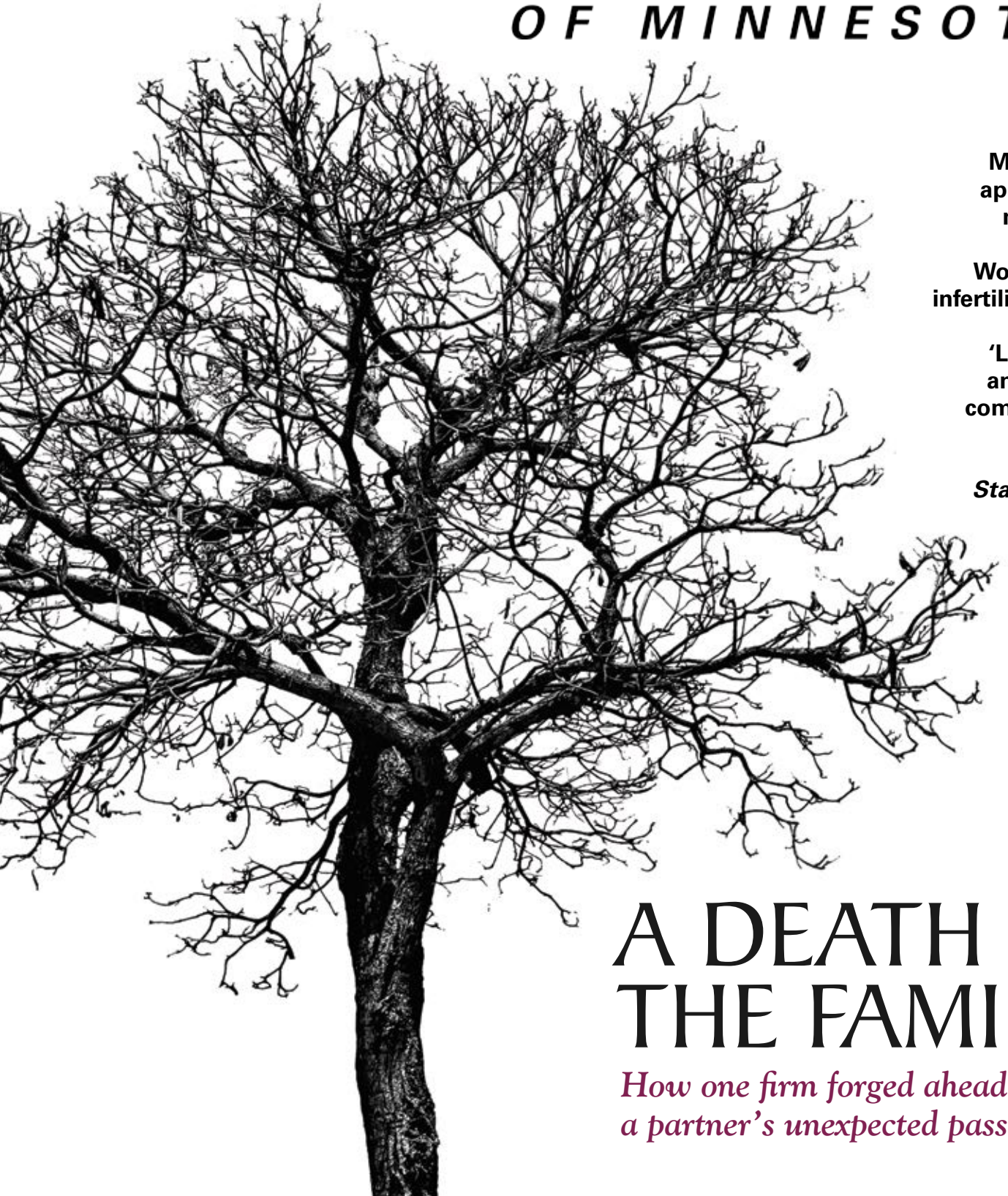
Being mindful of our social media activities can seem overbearing and perhaps a bit paranoid. Surely, a little Tweet can't be that big of a deal, right? Who cares? And maybe the majority of the time, nobody will care. But taking responsibility for the security of our organizations and firms requires an acknowledgement of the risks and threats that our digital lives present. With social media, people often end up their own worst enemies thanks to what they choose to share. Doxxing isn't always a complicated treasure hunt that requires carefully surveying multiple reseller websites. It can also be a quick trip to the potential victim's Facebook page. ▲

"Doxxing isn't always a complicated treasure hunt that requires carefully surveying multiple reseller websites. It can also be a quick trip to the potential victim's Facebook page."

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVIII NUMBER V
MAY/JUNE 2021
www.mnbar.org

Bench&Bar OF MINNESOTA



Minnesota's approval of a new Line 3

Working with infertility and IVF

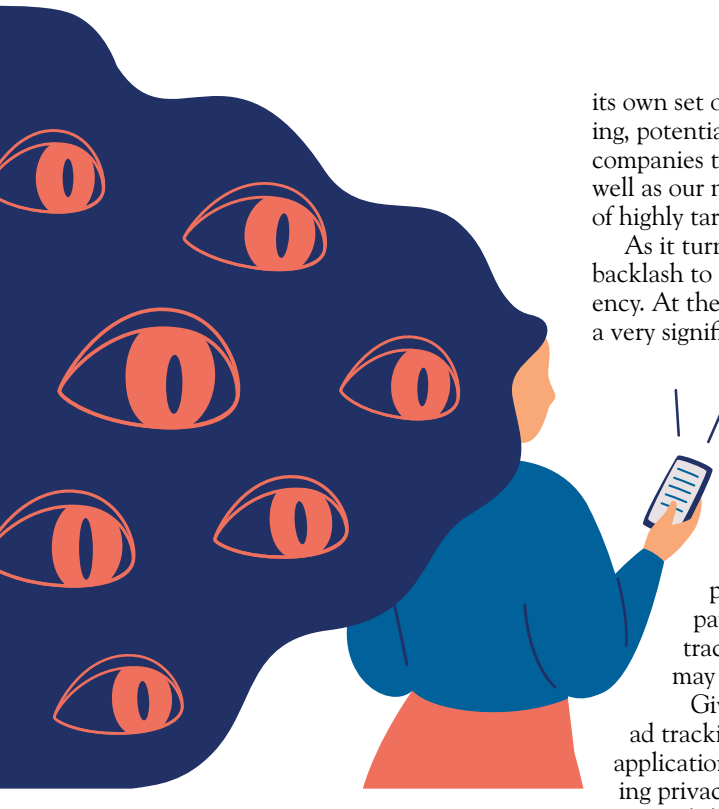
'Long covid' and workers compensation

Media got *State v. Khalil* all wrong

A DEATH IN THE FAMILY

How one firm forged ahead after a partner's unexpected passing

Apple's new iOS strikes a blow for data privacy



How many times have you found yourself discussing something with a friend or coworker only to see an ad for that very thing appear a few moments later? I, like many, have often had this bizarre experience and while it's easy to laugh these moments off as merely "creepy," it's remarkable to think about the vast amounts of data that are routinely collected about us. I was recently interviewed by CBS to discuss the often ignored reality that we allow huge amounts of data about us to be collected, stored, and traded every single day.[1]

Though many people actually like the convenience of customized ads, others see them as an invasion of privacy. I have often said that utilizing the many conveniences of technology requires a trade-off of our security, but the all-encompassing reach of the internet should give everyone pause. It turns out that downloading a variety of apps on our phones and mindlessly clicking our assent to all the terms and conditions comes with its own set of consequences—including, potentially, that we willingly allow companies to track our conversations as well as our movements for the purposes of highly targeted advertising.

As it turns out, there is a growing backlash to this obvious lack of transparency. At the end of April, Apple released a very significant update—iOS 14.5. Essentially, "app tracking transparency" allows users to accept or reject tracking activity on an app by app basis, but it also serves, in the words of a Wired article, to "simply expose how many apps participate in cross-service ad tracking, including some you may not have suspected."[2]

Giving users the power to deny ad tracking permission to particular applications is a huge step in preserving privacy. Apple has also recently created the privacy nutrition label, "requiring every app—including its own—to give users an easy-to-view summary of the developer's privacy practices… The privacy nutrition labels give users key information about how an app uses their data—including whether the data is used to track them, linked to them, or not linked to them."[3]

Though Apple's decision has many critics—Facebook is a primary opponent—the update underscores Apple's continued commitment to user privacy. Furthermore, the update still allows for customizable advertising by leaving the decisions to the individual. Apple's decision to support user control is certainly a step in the right direction. While no one measure can bring order and fairness to the mass data-sharing that goes on around us, it underscores the fact that users should have power to determine which personal information is shared about them, and with whom. Digital advertising isn't necessarily a bad thing, but it should be done transparently and with permission. Openly complying with data privacy regulations is essential for establishing trust with consumers, as an increasing number of individuals begin to pay attention to how their data is handled. In fact, recent data shows that since the update has been released, only about 4 percent of U.S. users have allowed apps to track them.[4]

While the United States does not currently have universal federal legislation related to data privacy or security, Apple's move may be indicative of a larger push to better establish and uphold user rights. Apple CEO Tim Cook has gone so far as to acknowledge data privacy as a fundamental human right, a position that other individuals and organizations are increasingly taking.

For the legal community, this movement highlights the raising of the stakes around data security. Even the largest organizations are now acknowledging the value of our personal data—and attorneys, as we all know, have a similar if not greater obligation to protect client data. Clients should always understand how their information is collected, stored, and protected. And those data privacy considerations must be taken into account when assessing the strength of internal cybersecurity measures. ▲

Notes

[1] *https://minnesota.cbslocal.com/2021/04/27/how-much-does-the-internet-know-about-us/*

[2] *https://www.wired.com/story/ios-app-tracking-transparency-advertising/*

[3] *https://www.apple.com/newsroom/2021/01/data-privacy-day-at-apple-improving-transparency-and-empowering-users/*

[4] *https://mashable.com/*

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXV NUMBER VI
JULY 2018
www.mnbar.org

Bench & Bar OF MINNESOTA

MSBA President 2018-19

PAUL GODFREY

A Coaching Style of Leadership

Stairway to Hell: Workers' comp decisions

The origins and evolution of the LPRB

2018 legislative session recap

Bankruptcy clawbacks

Social media and managing reputational risk

Recent events involving a certain television show remake and its quick and much-applauded cancellation have me ruminating on the repercussions of social media usage. In today's digital world, many of us feel pressured to keep up with the constant onslaught of information that presents itself to us on a minute-by-minute basis. Through any number of social media platforms, people now have free rein to express their opinions on everyone and everything. But this free rein does not mean that one faces no consequences for poor judgments, or that the informal nature of a tweet or post will mitigate the seriousness of the content. While reputational risk is often a difficult-to-quantify consequence of a data breach, it is also a consequence of our own digital actions.

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 trials. He is a member of the MN Lawyers Professional Responsibility Board.

Social media platforms tend to create the impression that, since the format feels fleeting and unofficial, so too is the content regardless of the sentiment being expressed. Not so. If anything, the speed with which social media allows us to communicate makes for swift and public consequences. ABC's decision to cancel the show in response to Roseanne Barr's offensive tweet was quick and deliberate and left no room for interpretation of her intent or excuses for her behavior (despite her attempts). Furthermore, given how quickly the tweet entered the public sphere, there was no time for anyone on Roseanne's public relations team to adequately respond or preemptively mitigate the damage. While many agree with ABC's prompt decision-making in this instance, the episode also stands as a cautionary tale about expressing oneself on social media. Though we may feel expected to act quickly on the internet, we should never be too hasty to express ourselves, especially not in writing.

It only *feels* anonymous

Social media is consistently treated as if it were yet another anonymous aspect of the internet. Even within organizational settings, there is a pervasive and groundless faith that only intended audiences are viewing what you post. Instagram, Facebook, Twitter, and sometimes LinkedIn are frequently treated as public diaries—where, for whatever reason, users feel entitled to privacy and are affronted when they realize that they are going to be held accountable for their words. Many use "free speech" as an excuse, but free speech does not protect individuals from facing consequences at work, including termination. We have all heard the horror stories about a boss discovering an employee's sick day fib when photos of him or her at a sporting event emerge on Facebook. But there is an entire range of social media-related problems that may include an organization facing blame for an employee's hate speech or racially discriminatory social media rants. In reality, we are hardly anonymous on the internet, and social media platforms give us a potentially very loud and public voice regardless of whether we were seeking one.

Social media ultimately offers little leniency when it comes to inappropriate posting, in spite of its seemingly anonymous and informal nature. When something is in writing, the results of an inappropriate comment being publicly shared online can be swift and long-lasting.

Instagram, Facebook, Twitter, and sometimes LinkedIn are frequently treated as public diaries—where, for whatever reason, users feel entitled to privacy and are affronted when they realize that they are going to be held accountable for their words.

Recognizing this fact is very important within the legal community, because of course clients and the public expect attorneys and law firms to maintain only the most ethical reputations. As a cybersecurity expert, I most frequently caution people against sharing their personal information online to avoid becoming victims of cybercrime and identity theft. But today it's also extremely important that we all be cautioned against publicly sharing any thoughts or opinions we would not be comfortable sharing with everyone. If you would not want a client, your neighbor, your boss, or a judge to read it, avoid posting it. As representatives of law firms, clients, and the law itself, those within the legal community are held to an even higher standard than other organizations and their employees.

Managing social media presence

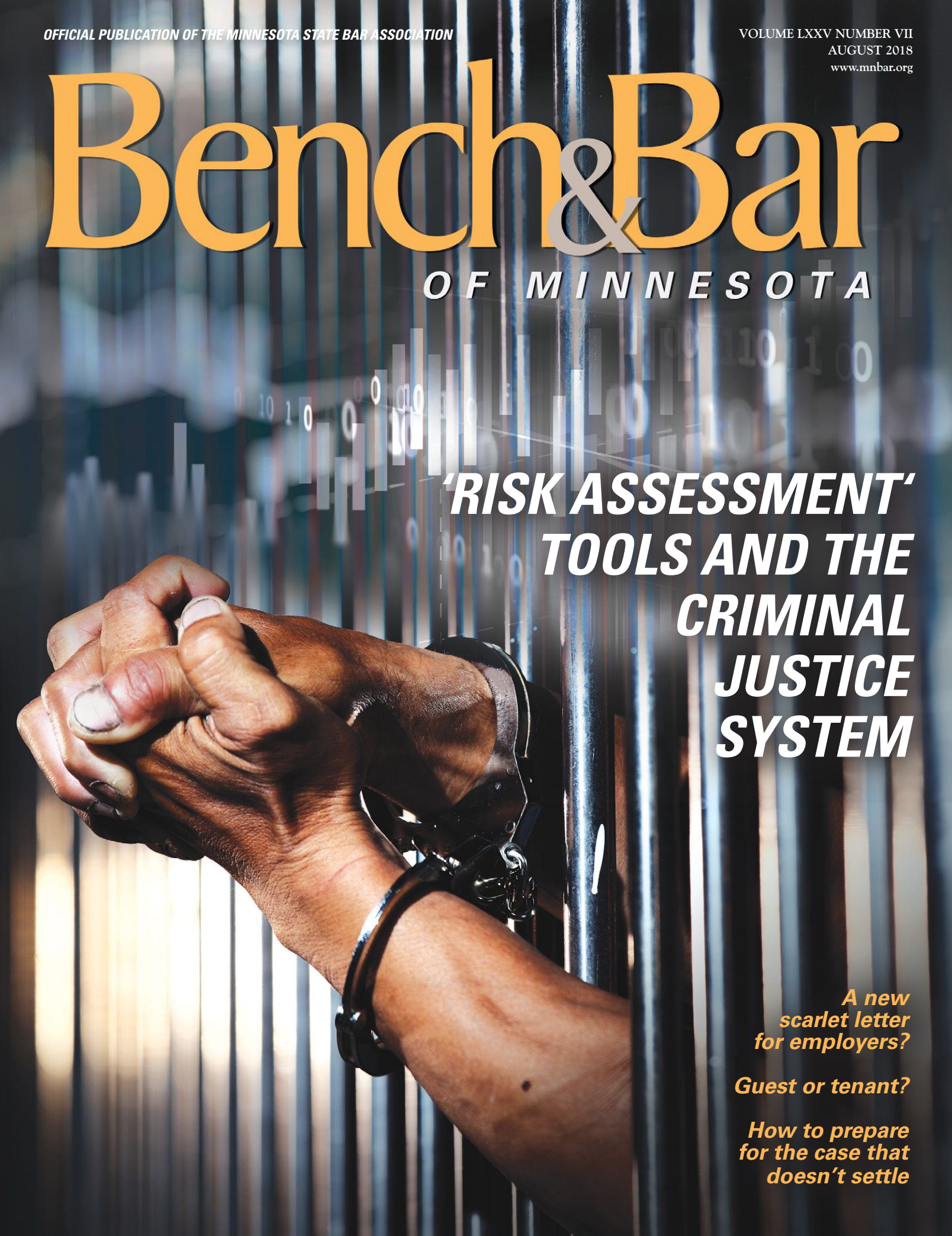
It's important that lawyers understand what is expected of them when it comes to managing their social media accounts. This seems to be a frequent point of confusion in the workplace, and with good reason. The distinction between public and private accounts, what is appropriate inside and outside of the physical office space, and what makes for a "bad tweet" all seem to be topics of debate. These topics seem to be particularly divisive among different generations of technology users. Upper management may struggle to appreciate the fact that newer hires have been raised on social media, and thus, it plays a different role in their lives. Trying to control posting may seem too heavy-handed for newer generations in the workforce, yet it remains the case that unchecked social media presence may permanently hurt an organization's public image.

Ultimately, nothing posted on the internet is ever truly anonymous. While a tweet may be posted and forgotten, the consequences that may follow are frequently long-lasting. Roseanne Barr's tweet cost her the revival of her show, her career, and arguably, her legacy. Social media missteps by attorneys can cause reputational damage to their firms and undermine their credibility with potential clients. Slowing down makes a world of difference when it comes to acting responsibly online. Instead of reacting immediately to the slew of digital information and provocation that's thrown at us every day, take a minute to carefully consider whether what you have to say is valuable and worded respectfully, and whether you would have a problem with any particular person reading it. ▲

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXV NUMBER VII
AUGUST 2018
www.mnbar.org

Bench&Bar OF MINNESOTA



'RISK ASSESSMENT' TOOLS AND THE CRIMINAL JUSTICE SYSTEM

A new scarlet letter for employers?

Guest or tenant?

How to prepare for the case that doesn't settle

E-discovery vs. forensics: Analyzing digital evidence

Digital evidence continues to be a growing focus of the legal community. In a very real way, digital evidence and its utilization in court can be compared to the advances in the use of DNA science that our courts saw in the last century. In a ubiquitously digital world, digital evidence has applications in almost every case, both civil and criminal. Like DNA evidence, digital evidence has the potential to be absolutely critical in the unfolding of a case. Unlike DNA, it presents the legal community with a moving target. As technologies change, the law has to keep pace with a continually evolving digital landscape. Furthermore, given users' individual usage patterns, no two cases involving digital evidence will ever be the same.

Internet-connected devices pose significant issues in using digital evidence and understanding the full scope of its applicability. We are no longer contending with just computers. Smartphones, cars, smart devices and appliances, software tools, the cloud, social media, fitness tools, and email are all kinds of data that may be utilized. With respect to all of these separate and yet interlocking technologies, the legal community is held to a very high standard in keeping up and making the most of all available information for their clients. One key aspect of the equation lies in deciding what route is best when it comes to collecting, storing, and ultimately presenting electronically stored information (ESI) in court.

E-discovery versus forensics

As of right now, e-discovery is the primary tool of courts and the legal community when it comes to the use of ESI in the courtroom. E-discovery procedures are quite different from digital forensic services. Each process is ultimately characterized by a different goal. Think of a filing cabinet that contains the files pertaining to your case. An e-discovery investigation is basically going to show what files are inside of the filing cabinet, in a broad format. A digital forensic investigation is going to identify the files as well. But, perhaps more importantly, a digital forensic investigation can also reveal the stories behind the files—who created the files and put them in the cabinet, what has happened to the files since being placed in the cabinet, when the files were created, who has accessed them, and whether any of the files placed in the cabinet are missing. In a digital forensic examination, this type of contextual information is paramount in the presentation of ESI as digital evidence.

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 trials. He is a member of the MN Lawyers Professional Responsibility Board.

This distinction in goals demonstrates the ultimate difference between the processes—namely, that digital forensic examinations seek to provide narratives of digital activity. E-discovery can offer legal teams a dump of digital information, but a forensic investigation offers an understandable, "translated" story. The best digital forensic experts are those who take the most complex technical findings and make them relatable within that framework. The power of the digital evidence will only be as strong as the testifying expert, whose job it is to construct a viable timeline out of objective ESI. E-discovery largely leaves the technical details and establishing the value of the evidence to legal teams.

While digital evidence can serve as a kind of objective witness, giving it a voice can be difficult. When the e-discovery process is chosen to gather such evidence, "getting it to speak" isn't even a consideration. This job is largely left to the recipients of the information, legal teams that may or may not be well-versed in technical language and the underlying value or meaning of particular pieces of data in the overall timeline of a case. The continuously changing nature of technology and ESI makes this an even more fraught issue.

No fishing expeditions

In addition to the possibility of needing a testifying expert for litigation, digital forensic analyses are helpful in preventing the kinds of ESI "fishing expeditions" that e-discovery procedures often end up pursuing. Protocols for forensic investigations should consider the scope of the analysis, including the number and type of devices involved in a case. This consideration is critical at the outset of a case, since collection and preservation should be conducted immediately. Protocols should also stipulate proper collection techniques, mechanisms for privilege review, cost sharing amongst the involved parties, reporting timelines, and the ultimate disposition of the data.

E-discovery and computer forensics are already fixtures in our legal process. Increasingly, people and companies needing representation use technology in a way that can affect the outcome of litigation. When most of our lives are in some way documented, especially within organizational settings, digital evidence can often be the most salient source of objective information. Our changing technological climate has forced the legal community to adapt to new rules and standards regarding data collection, preservation, and use in court.

Legal professionals have been further charged with understanding how, and to what extent, people use technology, especially as internet-connected devices document a new degree of connectivity and communication. Once attorneys are capable of recognizing the issues pertaining to digital evidence, they are better equipped to leverage computer forensic examinations in building their clients' cases. In some instances, forensics is becoming a necessity—a means of authoritatively establishing the arc of a case when human voices disagree or dissemble. Narratives of digital activity are much more valuable than heaps of unfiltered data. ▲

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVII NUMBER VIII
SEPTEMBER 2020
www.mnbar.org

Bench&Bar OF MINNESOTA

Covid-19 liability legislation

Force majeure *Hitz* home, excuses rent obligation

***Bostock v. Clayton County* and the future of the MHRA**

One Size Does Not Fit All

Estate planning for blended and nontraditional families

The Twitter breach and the dangers of social engineering

This past July, Twitter fell victim to a wide-scale cyberattack that compromised the accounts of some of its highest-profile users. It was soon determined that the attack was largely orchestrated by a 17-year-old boy, who apparently had a history of online scams—including some perpetrated on Minecraft—that amassed him a huge bitcoin fortune.[1] Twitter posted details about the attack on its blog: "The social engineering that occurred on July 15, 2020, targeted a small number of employees through a phone spear phishing attack… Not all of the employees that were initially targeted had permissions to use account management tools, but the attacks used their credentials to access our internal systems and gain information about our processes."[2] The post goes on to say that the attack focused on exploiting the human vulnerabilities that contributed to its success.

This episode underlines a simple truth that most cybersecurity experts acknowledge: The human element is what ultimately determines the strength of an organization's security posture. No degree of compliance or security budgeting can eliminate the potential for an attack on employees or staff themselves. As in the case of Twitter, once credentials were willingly offered up, the cybercriminals were able to access critical assets and compromise accounts.

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

Human vulnerabilities are always going to be much easier to hack than technology. In this instance, a 17-year-old boy was able to trick a number of employees at one of the largest tech companies in the world. And the scary thing about it is that it was relatively easy to do. So how do we mitigate some of this continuing, inescapable human risk?

One step that Twitter is taking is to more carefully manage access controls. Twitter has pledged that the company will be improving its procedures and policies to better monitor and restrict access to internal assets. Access controls are a critical piece of an organization's overall security posture. Limiting access to critical data, systems, and networks is a surefire way to mitigate some of the potential risk. The more an employee is able to access, the greater the liability that employee poses in the event of a compromise. Restricting and auditing access controls do not make employees immune to spear phishing attacks, but these measures definitely limit the damage if and when employees become victims.

Second, training and education are always going to strengthen organizational security, but in particular, employees should be reminded that avoiding hastiness is always important when dealing with digital communications. The Twitter hackers conducted their social engineering attack via phone, by convincing an employee that they were calling from the technology department and required their credentials to access a customer service portal.[3] It is important to communicate to employees how personal information will be requested, and to establish that following up in person is encouraged (or required) when a request for personal information has been received. While email is the standard phishing method, it is important to remember that phone calls and texting can also be used to gather information. If anything appears suspect or out of the ordinary, make sure that reporting procedures are in place and that all employees know the designated communication channels. Taking a moment to slow down before acting on a request may make all the difference.

Like all high-profile breaches and cyber events, the Twitter breach should inspire organizations, firms, and companies to take a closer look at their own security postures and implement positive change. Security cultures thrive with top-down management support and a company-wide awareness that security is everyone's responsibility. ▲

Notes

[1] *https://www.businessinsider.com/twitter-hacker-florida-teen-past-minecraft-bitcoin-scams-2020-8*

[2] *https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html*

[3] *https://www.nytimes.com/2020/07/31/technology/twitter-hack-arrest.html*

Compliance & Ethics Professional®

April 2016

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Mark Lanterman

Chief Technology Officer
Computer Forensic Services
Minnetonka, MN

See page **14**

29
EU Data Protection Regulation: Are we nearly there yet?
Jonathan P. Armstrong

33
Marketing and Data Security Practices: The *FTC v. LifeL ock* settlement
Keith M. Gerver and Peter T. Carey

39
"To disclose, or not to disclose? That is often a tough question."
Peter Anderson

45
The Ethics Wheel: Shaping corporate culture
Susan Korbal

an interview by Adam Turteltaub

Meet Mark Lanterman

Mark Lanterman (mlanterman@compforensics.com) was interviewed in January of 2016 by **Adam Turteltaub** (adam.turteltaub@corporatecompliance.org) VP Membership Development at SCCE/HCCA.

AT: Cybersecurity is a bit of a nightmare issue. We just did a survey among compliance professionals, and they named it one of their top areas of concern for 2016. It's not surprising, given the headlines. I also well remember a couple of years ago at the Compliance and Ethics Institute when the Director of the FBI gave a scary talk on the topic. Is the risk getting greater or smaller?

ML: That's a good question. The best answer I can give is this—it's all proportional. By that I mean, the threats are no doubt growing in size and scope. As we come to rely more and more on technology, the bad guys are seeing more and more potential to steal and line their own pockets. By its nature, cyber threat intelligence is always a step behind the bad guys. Therefore, the risk is definitely one that is growing and will persist well into the future. Luckily, though, awareness and the market for digital security are also growing.

AT: One of the things that I find most troubling about this issue is that there are so many potential intruders. You could have a hacker wanting to access your system for fun or malicious reasons, state actors and competitors looking for trade secrets, and let's not forget employees with a grudge or who are just careless. How would you prioritize the risks among these and other potential sources of breach?

ML: Motive is important in analyzing and understanding cyber breaches in order to prevent them. However, I don't think it should matter what a hacker's motive may be. Every breach should be treated as a malicious, serious, and potentially damaging threat. That said, the nature of different threats, and consequently, the potential damage of a breach, is really dependent on an organization's digital infrastructure. Thus, organizations are really in the best position to rank these threats for themselves. We have certainly seen that different organizations are in different spots on the spectrum.

Our primary observation over the years has been that data breaches occur because of a simple lapse of judgement. The single most important aspect of security is people.

AT: Are there specific strategies that companies should employ to counter each of these threats? If so, what would they be?

ML: While there are specific measures that organizations can take, it is highly dependent upon the variables in a given organization. In other words, there is no "one size fits all" for a strong digital security plan. Furthermore, the technology changes on a daily basis. The most secure companies are the ones that do not let their security plans grow stagnant. The best are those that account for changes in the technology, educate employees, and audit consistently.

AT: What do the strategies all have in common? Put another way, what should every company be doing right now?

ML: Our primary observation over the years has been that data breaches occur because of a simple lapse of judgement. The single most important aspect of security is people. The human element of technology is just as, if not more, important than the tech itself. It can only ever be achieved through education and strong implementation of written digital use policy. I like to refer to this as fostering a "culture of security." Therefore, I think that companies should be educating their employees on a regular basis about the realities of digital attacks, how to recognize them, and what to do in the case that something does happen. Such education programs should cover everything within the company's digital security policies—from mobile devices, to social media, to passwords and encryption and backups.

AT: What are some of the common mistakes you see companies making when it comes to shoring up their cyber defenses?

ML: I think the biggest mistake I have seen is over-confidence. Many organizations believe that they have done all they can to prevent a breach, and are thus absolved from putting in place any sort of contingency plan should a breach occur. These organizations adopt a posture of: "Something like that cannot possibly happen to me." When breaches

happen, too often the C-suite executives are caught looking like deer in the headlights. As the old adage goes, "Hope for the best, but prepare for the worst." Therefore, I recommend that an organization take the time to delegate roles and responsibilities and have a plan of action should its worst fears be realized.

AT: Compliance officers are increasingly getting involved, if not taking charge, of this aspect of IT. What's the first thing a compliance officer should look for when assessing the risk of cyber attacks, and their company's defenses?

ML: Compliance officers have an interdisciplinary job. They need to educate themselves not only about how the different technologies within their organization's network, but more importantly, they need to understand how those technologies are being used. I advise compliance officers to remember one key fact: No hacker (unless you have been breached already) knows more about your organizations digital infrastructure than you. Compliance officers have the potential to learn everything there is to know about an organization's digital and non-digital assets. I recommend that compliance folks take the time to not only learn the tech, but also use their discretion to prioritize which assets need the most protection.

AT: How much does a compliance officer need to "get into the weeds" of security protocols and other technical factors? Is it time to get some training, or best to leave the technology decisions to the experts?

I advise compliance officers to remember one key fact: No hacker (unless you have been breached already) knows more about your organizations digital infrastructure than you.

ML: In order to effectively manage and audit digital security, compliance officers should absolutely have a general understanding of the technology to a point where they would feel comfortable with the jargon between Legal and IT in the event of a breach. It is important to know about what happened in order to report it and prevent it moving forward. As far as "getting into the weeds" or minutiae of the technologies, I don't think that is necessary. I think the best compliance officers know that when it comes to digital security, outside vendors and digital security contacts are absolutely necessary in most cases, no matter how many details a compliance officer knows about the tech.

AT: You do a lot of computer forensic work, which leads to another area of cybersecurity: making sure you aren't holding onto documents longer than you should. Are companies getting better about their document retention practices? Or do they still have policies and haven't gotten to the real putting-them-into-practice stage?

ML: That is an excellent point. Document retention practices are actually a key aspect of digital security. Keep too much for too long, and you have that much more information that can potentially fall into the wrong hands. Keep too little, and there may be serious inconvenience factors, costs, and other issues. A good security plan always accounts for the volume and type of data that is available. More importantly, it also addresses where the most important digital assets are located,

so that the proper resources can be diverted to an organization's "crown jewels." But this question is really dependent on the policy choices an organization and, perhaps in some cases, what an industry's standard dictates.

AT: I remember a few years ago there was a lot of press about companies getting rid of old photocopiers and not realizing that thousands of their documents might be stored on them. I imagine most have gotten better about that, but should compliance officers be worried about all the old laptops and smartphones hanging around? Are they being disposed of properly?

ML: As much as the industry should be concerned about external attacks, it is important to not forget about the smaller, seemingly innocuous security lapses. Data exfiltration from negligence happens all the time, which is a shame, given how easy it is to prevent. Think about a breach in the form physical device theft. For instance, as you know in the healthcare industry, data breaches that affect 500 patients or more must be reported to the U.S. Department of Health. Hundreds of reported incidents involve stolen laptops and phones. With theft, there is clear evidence that data has been stolen. In the case of disposal, companies often fail to securely wipe data before selling or recycling. Failing to recognize this, these types of breaches would never be reported, as no one would expect anything to be wrong.

AT: That leads to one last area to explore: smartphones. These days most everything is kept on them. How secure are they? What should compliance officers be asking their IT teams to make sure that they truly are secure?

ML: Mobile devices have changed how work gets done. While they are often secure, it all depends on how they are used. There are always threats that are unique to mobile computing. For example, like public restrooms, public Wi-Fi should never be trusted like your own. Public Wi-Fi networks are very useful, but there is always a risk in using them, because they can be a portal for cyber criminals to steal your valuable data, including usernames and passwords. This alarming trend is what is known as a "man-in-the-middle" attack. Essentially, this kind of attack enables a hacker to eavesdrop on your Internet connection, intercept your communications, and in some cases, reroute your connections to their own malicious webservers and material. For many websites you may visit regularly, a hacker can remove the encryption from the websites' secure login pages. Again, there is always the persistent and very real increased risk of device theft, not just of smartphones, but all mobile devices. Considering all this, I would suggest that compliance officers ask IT about public Wi-Fi use prevention and data encryption. With encryption, data on mobile devices is rendered inaccessible to a thief.

There are always threats that are unique to mobile computing. For example, like public restrooms, public Wi-Fi should never be trusted like your own.

AT: So, once the company-issued devices are covered, that's only halfway there. There are still the personal devices that employees are using. What protocols should be in place if a company has a "bring-your-own-device" policy?

ML: Unfortunately, in most instances, bring-your-own-device (BYOD) relinquishes some defined, universal security strategy, and inherently gives an organization less in the way of data control, because standard mobile device management tools are not used with employee's personal devices. Many smartphones also offer device tethering, whereby the phone's cellular data connection is shared with other devices. This type of network activity is not monitored. Before simply accepting BYOD as a cost effective and desired approach, ensure that policy is clear and consequences are clearer. Also consider with Legal whether there are special regulatory concerns particular to a certain industry. In some industries, like healthcare for example, such a lack opens up serious liability.

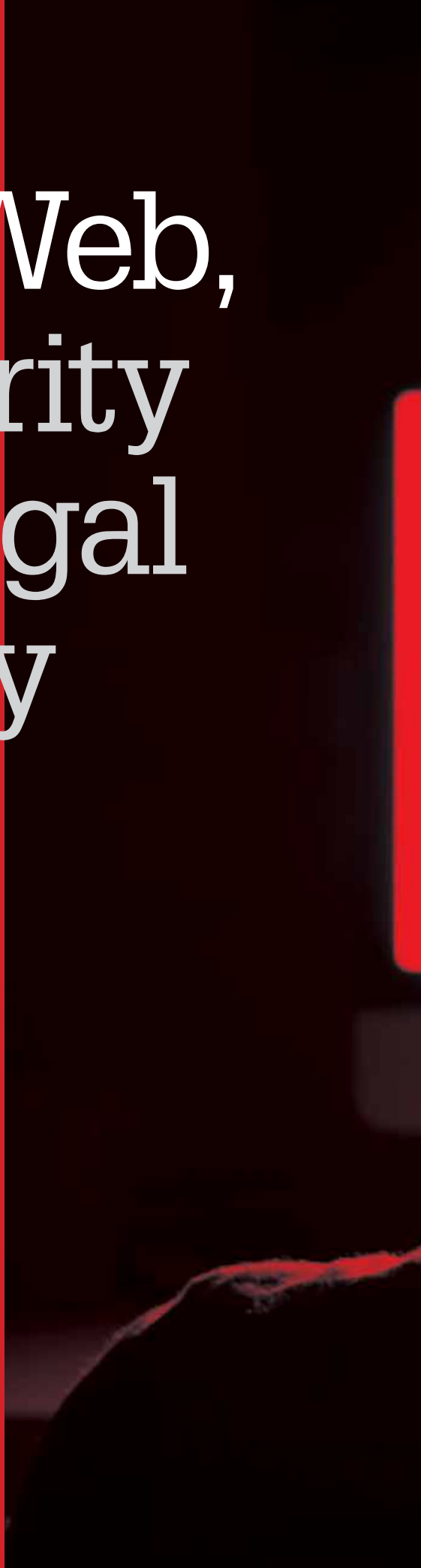
Beyond BYOD, I also urge compliance professionals think about BYOC (bring your own Cloud). The risk with BYOC is two-fold. First, it can be an avenue for disgruntled employees to easily take information with them after leaving. Second, they also pose unique mobile security risks. Interestingly, rather than stealing a username and password, cybercriminals have found a way to steal and use password "tokens" that are stored with a Cloud application on a user's mobile device. These tokens store a user's credentials for convenient access from a trusted device, making it so a user does not have to re-enter a username and password each time they access the app. By using other types of attacks, such as Wi-Fi exploits or a phishing attack, this credential token can be stolen and used to authenticate another untrusted device. Since this token is unique to a legitimate "login" session, it makes detection difficult, and even the service providers will have a hard time detecting the compromise.

AT: Finally, given the threats out there, is it time to start asking a very hard question: Should some of our data NOT be available through our network? Is there some data that's safer if we keep it offline on a desk somewhere?

ML: That is a very hard question and not one I can answer for everyone. It is all about finding that magic recipe that balances convenience with security. It is important to remember that there is no such thing as perfect security, no matter where or how data is stored (whether digitally or on paper). Just because it's not connected to a network does not mean it cannot be stolen. In many ways, storing information digitally allows for greater control of access privileges.

AT: Thank you, Mark for sharing your insights with us.✳

The Dark Web, Cybersecurity and the Legal Community



As technology advances and capabilities grow, so does the number of evolving threats.

By Mark Lanterman

From lightbulbs, cardiac devices and washing machines to the instant communication our smart devices offer, the internet of things (IoT) has impacted nearly every facet of our personal and professional lives. These capabilities offer us unprecedented levels of convenience but also an unprecedented number of evolving threats and a complicated interplay of risks that require constant diligence and attention.

As IoT continues to pervade how organizations operate, the legal community must adapt to uphold the highest standards in protecting client data and operational integrity. With tasks ranging from considering cyber liability insurance policies to budgeting appropriately in reactive and proactive cybersecurity practices, counteracting the magnitude and variety of cyber threats that the average firm faces can seem like a daunting task.

THE RISE OF THE DARK WEB

Often considered to be a "far away" threat, the risks associated with the dark web are often underestimated. The internet that most of us know—Amazon, email, retail websites, news sites and social media—only accounts for a small fraction of the entire internet. The dangers lurking in the dark web are like the deepest parts of an expansive and mostly unknown ocean, with regular internet browsing patterns represented by a clearly visible and accessible shoreline.

For the legal community, the dark web presents several risks, many of which aid a cybercriminal in executing attacks. From information gathering in the wake of a breach to opening credit accounts using purchased card numbers, cybercriminals rely on the dark web.

Clients expect the utmost care in ensuring the confidentiality of their data. Law firms are prime targets of cybercriminals because of the value of the data they collect and store. In this article, I will discuss some of the primary threats that a firm may encounter, the types of risk associated with these threats, and steps to both prevent and mitigate damages in the event of an attack.

ADDRESSING MALWARE

One significant risk for law firms is the installation of malware via social engineering attacks. "Malware" is bad software that is installed by bad actors with the intention to exploit vulnerabilities in code, which allows for other forms of software on the targeted systems to act the way the cybercriminals want it to. Once malware is installed, data exfiltration, operational dysfunction, control of the device by the cybercriminal or ransomware attacks can all ensue. Viruses, worms, rootkits, ransomware and spyware are all types of malware that can be installed in a variety of ways, and all pose significant risks to a law firm. However, the primary method that cybercriminals tend to utilize in disseminating malware is social engineering.

Social engineering attacks take advantage of the all-too-forgotten "human" element of security. Instead of compromising technological weaknesses, cybercriminals will go for a route that typically takes a lot less work. Phishing emails are probably the most common social engineering tactic. A typical phishing email appears to be sent from someone we know, maybe a boss or co-worker. The email will often request a confidential task that needs to be done right away. "I am busy right now and can't talk on the phone. I need a $50,000 wire transfer. This needs to be done immediately, so don't tell anyone about it. Thx." When the request seems urgent and especially if it appears to be coming from upper management, an employee may feel pressured to follow through without double-checking or ensuring the validity of the demand. These emails can often appear legitimate, including details that would at face value seem to only be known by the sender.

Social engineering attacks are often strengthened and personalized by a method known as doxxing. Doxxing is the act of publicly identifying or publishing private information about a person, often with malicious intent. To strengthen an attack by personalizing it to the target, a cybercriminal will frequently visit personal information reseller websites to gather as much information possible. The dark web may also be a source of information.

Perhaps more damaging though is information willingly put out on the internet by the targets themselves. Social media can be a cybercriminal's best source of information. Posting personal information, even something as innocuous as when you are going to be out of the office on vacation, can be used to bolster a social engineering attack and result in data exfiltration, financial damage or reputational

Law firms are prime targets of cybercriminals because of the value of the data they collect and store.

harm. Legal consequences can also ensue, as well as operational dysfunction.

THE RISK TO LAW FIRMS

The risks associated with cyberthreats are both immediate and ongoing and extend far beyond a firm's financial strength. An attack that compromises the confidential data of a firm's clients can severely impact that firm's reputation and overall success. In our digital age, the legal community has the huge responsibility of ensuring the confidentiality of its clients' digital information. Any breach in this trust is going to have immediate and long-lasting repercussions.

Cyber attacks also pose significant financial and operational risks. Responding to an attack, especially if a firm has no pre-existing plans or protocol in place, can be incredibly expensive and time-consuming. A ransomware attack that requires financial payments to regain access to client data can cost a firm thousands of dollars.

Operationally, an attacker may gain access to a firm's devices, making day-to-day operations impossible to conduct for a period of time. The ongoing legal risk associated with an attack, especially in the event of client data being compromised, can further contribute to a firm's financial losses and reputational damage.

PLANNING AHEAD

To counteract these threats and mitigate the associated risks, thinking ahead is a firm's best approach. Combining proactive and reactive cybersecurity strategies is critical, as well as designating in-house parties responsible for cybersecurity and ensuring top-down management support of security protocols and procedures. Proactive cybersecurity strategies include the development of a cybersecurity team responsible for ensuring the development and implementation of cybersecurity standards, and the establishment of clear communication channels in the event of a cyber attack.

Moving beyond the IT department, creating a culture of security requires interdepartmental support, especially from upper management. If an employee receives a phishing email, he or she should know how to (or not to) respond and how to report the incident to appropriate parties.

Proactive solutions should also consider best practices in regard to email encryption, fortifying networks, implementing controls, the security of third-party vendors, physical security, the institution of regularly scheduled security assessments that include vulnerability scanning as well as penetration testing and employee training and awareness programs.

Part of a proactive cybersecurity approach is that a firm knows how it will respond in-house and publicly if it is made victim to an attack. Having a third-party security vendor on hand for assessment and mitigation is often a necessary first step; gathering accurate information about the scope and damages of a breach is important in addressing the public and mitigating ongoing damage. Reporting procedures and requirements should also be understood prior to an incident occurring.

Our interconnected world has made things easier but also more complex. When technology works in our favor, it makes everything better. Data can be collected and stored easily and in huge amounts, communication is instant and the operations of our organizations are made possible. Credit freezes and good "cyber hygiene" may prevent some of the dangers associated with the dark web and the personal information that may be readily available there. When cybercriminals take advantage of technology, the results can be disastrous, especially within the legal community. Acknowledging the ever-evolving threat landscape, as well as its associated risks, can help keep a firm one step ahead. **LP**

Mark Lanterman is the founder and chief technology officer of Computer Forensic Services. Before entering the private sector, Mark was a member of the U.S. Secret Service Electronic Crimes Taskforce. He has testified in over 2,000 cases. **info@compforensics.com**