AMERICAN BANKRUPTCY INSTITUTE

2021 Consumer Practice Extravaganza

Easiest Catch: Don't Be Another Fish in the Dark 'Net

Mark Lanterman
Computer Forensic Services; Hopkins, Minn.

Jon J. Lieberman
Sottile & Barile LLC; Loveland, Ohio

CONCURRENT SESSION

2021


OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION
VOLUME LXXVII NUMBER V
MAY/JUNE 2020
www.mnbar.org
Bench&Bar
OF MINNESOTA
LAWYERS, INTERRUPTED
Learning to practice in a pandemic

Law&Technology | BY MARK LANTERMAN

Working from home and protecting client data

In recent days, remote work has become the norm in the legal community. Teleconferencing, email, and myriad digital communication methods are even more important now than they were before the covid-19 pandemic. This abrupt shift requires consideration of ethical obligations when sending and receiving client data and personal information electronically. It's especially critical now, since many organizations had to rush to get proper remote work infrastructure in place, emphasizing convenience and operationality over security protocols. The legal community is held to a particularly high standard when it comes to protecting client information, and is therefore required to stay apprised of best practices in cybersecurity. Referring to the CIA triad—a security model that focuses on the confidentiality, integrity, and availability of data—is helpful as we work to optimize security and efficiency in our remote work environments.

According to the ABA Standing Committee on Ethics and Professional Responsibility's Formal Opinion 477R:

> A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

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.

This requirement acknowledges that using technology is imperative for efficiency and ease of communication with clients. But it also maintains that lawyers must have a degree of technical proficiency and knowledge of cybersecurity best practices. Lawyers must do everything in their power to protect the confidentiality of client data, and to make sure that in the event of a compromise, data would still be accessible. The confidentiality, integrity, and accessibility of client data is paramount as the legal community continues to work at offsite locations.

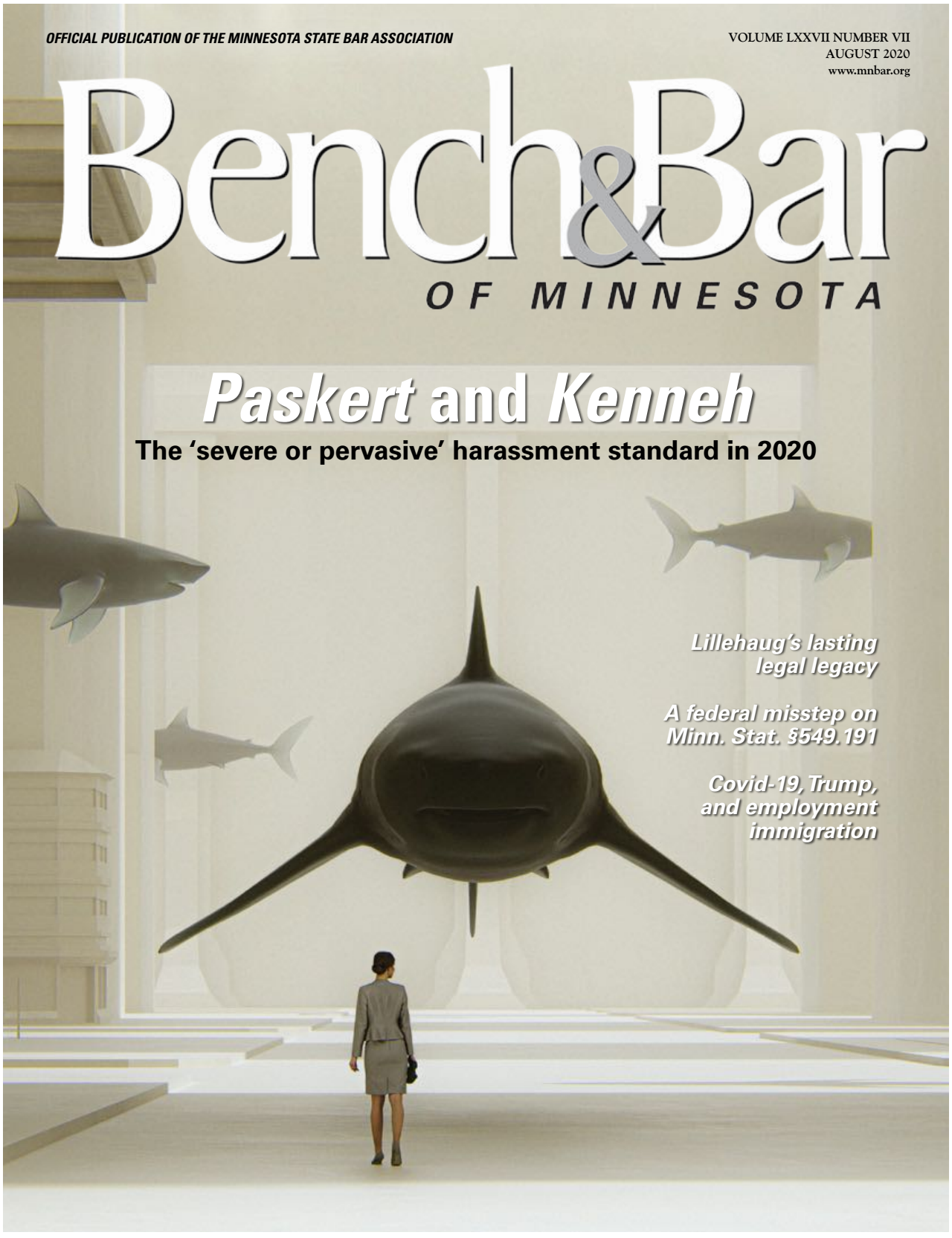
Though the situation is challenging, now is not the time to shrug off poor security practices. Relying on email disclaimers such as "If you are not the intended recipient of this email, please delete" is not enough to ensure the confidentiality of client data. Shifting blame from the sender to the unintended recipient is not an acceptable security strategy. Instead, standard email encryption policies protect client data by making data unreadable until it is "unlocked" via a decryption key. Use of VPNs, strong passwords and multi-factor authentication, avoiding public wifi, and securing endpoints are all a few ways that remotely working attorneys can protect their clients. Other important steps in securing remote work environments: avoiding suspicious websites or links, updating software when necessary, and making sure to only use approved technologies (such as known USB devices or hard drives). Each remote device in your network is essentially another gateway, another potential access point for an attacker; the covid-19 pandemic has brought about a number of nasty attack campaigns for which we should all be on the lookout.

Training on phishing scams and social engineering attacks helps to mitigate some of the threat, as these attacks are regularly conducted through email. As cyberattackers continue to take advantage of covid-19, staying apprised of potential cyber threats is an element of cybersecurity awareness that is required of attorneys. Slowing down can make all the difference when it comes to becoming a victim or spotting an attack. If an email seems strange, unexpected, or urges you to act quickly in a way that violates standard procedures, think twice. Communicating any suspicious activity while working remotely helps to prevent breaches; it also helps to inform clients of when they can expect communications and what they will contain.

Just as client data must remain confidential, ensuring its integrity and availability are top priorities. Managing access controls in-house lessens the risk that client data will be inadvertently (or purposefully) altered or destroyed. Make sure that the IT department is performing regular backups in a sound manner, and that system upgrades are being conducted when necessary. This pandemic has brought about a high number of cyberattacks, especially against those organizations that were underprepared for remote work and are now even more vulnerable. Denial-of-service and ransomware attacks can leave an organization unable to operate for an extended period of time. Having a backup plan protects against the financial, reputational, legal, and operational risks that come with a cyber event.

In many ways, cybersecurity is now more important than ever. Given their reliance on digital devices and communication, attorneys should take special note of their ethical obligations in dealing with client data. Remote work security strategies should be communicated to clients, as well as how they should expect to be contacted during covid-19 (establishing, for example, what types of information will be transmitted via email). Moving out of our physical work spaces does not mean that we can ignore the security protocols governing how we use technology in the office. If anything, additional layers of diligence and information-sharing should be added to account for the complex threats we now face.

Going above and beyond those "reasonable efforts" is necessitated by the extraordinary working situation in which many of us find ourselves. Maintaining a strong personal cybersecurity posture may help to ease some of the risks that a reliance on remote work introduces; it may also ease the minds of clients during a time when many things seem uncertain. ▲


OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION
VOLUME LXXVII NUMBER VII
AUGUST 2020
www.mnbar.org
Bench&Bar
OF MINNESOTA
Paskert and Kenneh
The 'severe or pervasive' harassment standard in 2020
Lillehaug's lasting legal legacy
A federal misstep on Minn. Stat. §549.191
Covid-19, Trump, and employment immigration

Law&Technology | BY MARK LANTERMAN

Cyber risk:
Is your data retention policy helping or hurting?

This past June, several U.S. law enforcement agencies were the victims of a largescale data breach resulting in 296 GB of data being stolen. The National Fusion Center Association stated that "dates of the files in the leak actually span nearly 24 years—from August 1996 through June 19, 2020." The statement went on to say that personally identifying information was leaked along with other types of files.[1] The incident was an act of hacktivism and purportedly sought to reveal internal government workings to the public, including details relating to its covid-19 response.

This incident reveals a critical piece of cybersecurity strategizing that sometimes gets overlooked—the value of the data retention policies. Data retention policies outline what types of data are actively being stored, how long that data should be stored, and how it should be destroyed or relocated at the end of that time. Part of the severity of this attack stems from the fact that these agencies were retaining so much old data—data that should have been periodically audited and reviewed. While data is a critical asset, only retaining what is absolutely necessary mitigates the risks associated with a breach.

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.

Within the legal community, attorneys are held to a high standard when it comes to protecting client data. And one size does not fit all: It's complicated knowing when it is appropriate to discard old client files, especially given ethical requirements and the possibility you'll need certain case files in the future. Depending on the jurisdiction, retention policies—and the length of time attorneys are required to hold on to files—may vary. Furthermore, different types of cases and circumstances require different approaches to file retention. A records retention schedule may spark fears that files will be deleted or discarded before it's appropriate to do so. But law firms are also likely to run the risk of holding on to more information than necessary, and for an indefinite period of time.

Creating a legally sound records retention and destruction policy better protects clients from having their information compromised. Essentially, the less data a law firm houses on its servers (or in their storerooms, in the case of paper copies), the more able they are to manage and secure that data. Communicating the records retention policy to clients helps to protect against prematurely deleting client information. In the File Retention booklet distributed by Minnesota Lawyers Mutual, it is recommended that a letter notifying the client be sent prior to its scheduled deletion or destruction date: "The letter should tell the client they are welcome to pick up their file, in its entirety, before a certain date and that failure to do so will result in the file being destroyed. It is also a good practice to include a 'consent to destroy' form."[2] This measure provides an added layer of caution in executing a firm's data retention policy while still working to minimize the amount of data that a firm retains on behalf of its clients.

It should also be noted that the digital destruction of files is more complex than pressing the 'delete' button. Best practices should be followed in forensically destroying data, and any files that are deleted should be recorded for future reference.

While regularly reviewing stored data and creating a record retention policy is important in mitigating the risks associated with data breaches, it remains true that firms are often required to store large amounts of data even for cases that have closed. The key steps in creating a cybersecurity culture focused on protecting client data include: access controls to sensitive data; encryption; and employee education and training about social engineering and the threats associated with the Internet of Things. Appropriate physical security measures should be enacted to best secure physical files and storerooms. While data is a critical asset in any organization, the legal community is especially tasked with safeguarding its data and managing it with the utmost care. Implementing a data retention policy is an important part of that effort. ▲

Notes

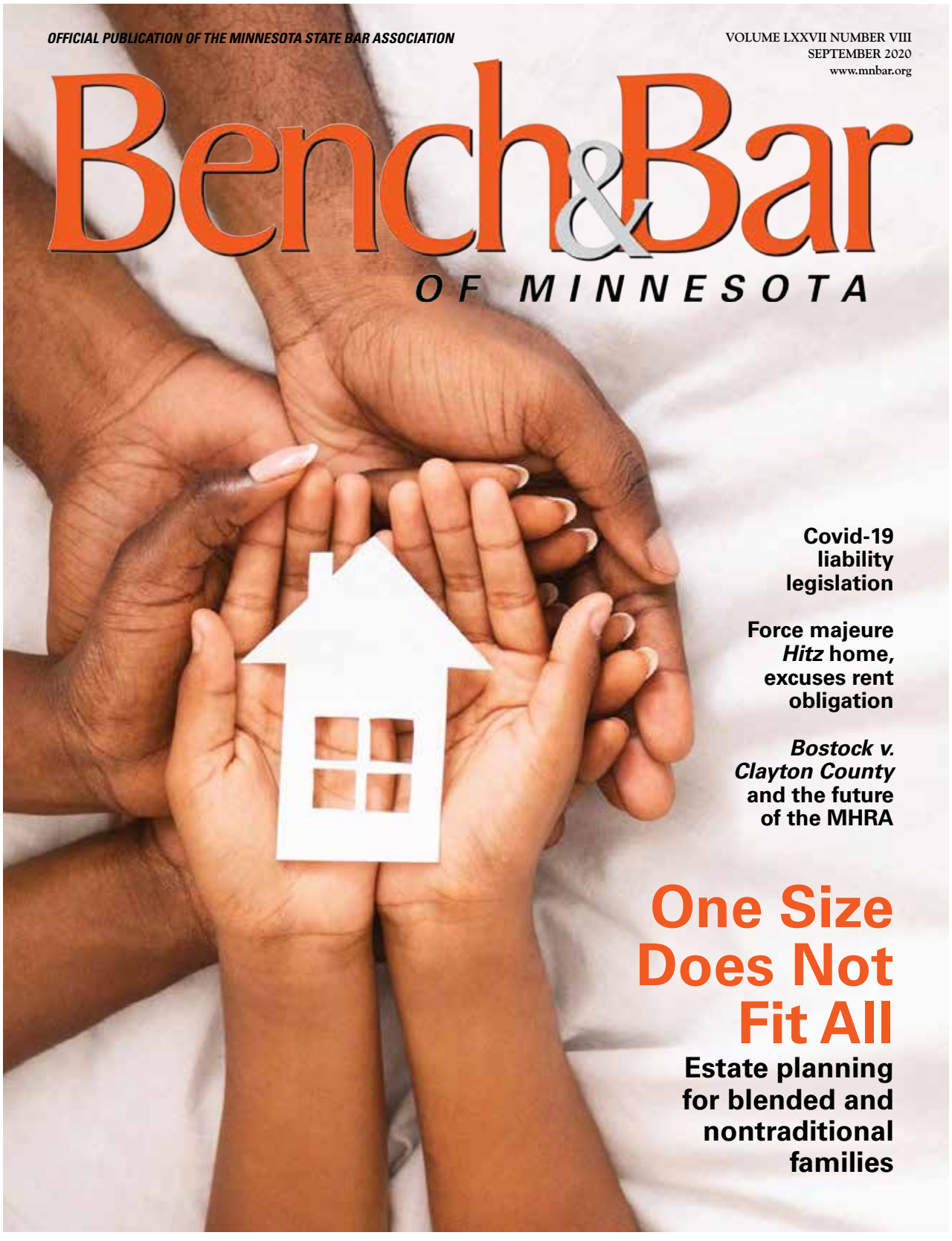
[1] *https://thehackernews.com/2020/06/law-enforcement-data-breach.html*

[2] *https://www.mlmins.com/Library/File%20Retention%20Booklet.pdf*

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

Law&Technology | BY MARK LANTERMAN

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*

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVI NUMBER III
MARCH 2019
www.mnbar.org

Bench&Bar OF MINNESOTA

ABA Formal Opinion No. 483, data breaches, and you

Substantial completion and liquidated damages

An interview with Justice Paul Thissen of the Minnesota Supreme Court

The Music Modernization Act, explained

Law&Technology | BY MARK LANTERMAN

Third-party vendors and risk management

It's always scary to think that sometimes data breaches aren't the result of "hacking" so much as user error. Rubrik, a security and cloud management firm, recently learned this the hard way, when a misconfigured server exposed data belonging to major clients.[1] As organizations use increasingly complex technology to handle increasingly vast amounts of client data, it is becoming more and more difficult to keep up with security demands.

As Rubrik was recently reminded, security demands include proper configuration and hardware setup as well as more advanced security measures of the sort I have mentioned in previous articles. Many organizations overlook the fact that third-party vendors can cause just as much damage in the event of a breach as an internal cybersecurity event. Reputationally, operationally, and financially, where the breach originated doesn't matter as much as who the breach is going to impact most. If the answer is an organization's major clients, I am willing to bet those clients won't care either.

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.

Managing third parties

Most organizations have some degree of third-party involvement in managing internal systems and cloud services, or in helping conduct some operational function. When entering into agreements for these services, it's advisable to have a designated person who is responsible for overseeing the agreement process and guiding the management and review of third-party risk. All third-party vendor relationships come with a degree of risk, regardless of the service they are providing. In the massive Target data breach of 2013, it was a third-party that compromised Target's data, affecting millions of its customers. Keep in mind that this third party provided HVAC and refrigeration services.[2] It goes to show that regardless of the company, third-party involvement always comes with dangers and requires continuing oversight past the initial stages of the agreement. Cyber risk management calls for separate ownership of different levels of risk, including third-party relationships.

Once a responsible person or group is designated for the management and overview of third-party relationships, one key task is to keep track of where organizational data resides. Record where the data is being stored, what type of data it is (especially if it's highly confidential or protected), and how the data is being protected by each vendor. Try to limit which vendors have access to sensitive data and incorporate ongoing reviews and audits as part of continued due diligence. Prior to entering into any new agreements, thoroughly research the prospective party's stance on cybersecurity issues and how they have handled any past incidents. What controls are used for sensitive data and who has access to systems? Do they audit their third-party subcontractors? Do they have an incident response plan? Is it readily available for review? Does it comply with the standards of the internal response plan in place? Asking the right questions can help determine whether the value of a third-party agreement is worth the risk from the outset.

Assessing risk

Service-level agreements should be created in compliance with the same security protocols and policies that regulate internal operations. When an organization trusts an outside source with its data or allows it access to the organization's networks, that source is now an element of its risk profile. If that vendor is vulnerable, so are you. If that vendor has a weak security posture, so do you, no matter how stringent your internal policies are. In addition to the reputational, financial, and operational risks that may be incurred from a third-party security incident, legal risks must also be taken into account—especially in light of HIPAA and GDPR regulations. Transparency about reporting data breaches is critical when it comes to working with third-party vendors; immediate notification of cyber events should be a stipulation of any agreement. Contractual considerations should include access requirements, reputation of the third party, liability, audit procedures, and termination of access to data when the agreement is cancelled or expires.

It is impossible to ensure perfect security, but organizations can take measures to mitigate the risks associated with advanced technology systems and growing volumes of data. Whether it's ensuring proper configuration of systems or controlling access, third-party vendor agreements introduce another element of risk to your organization that may be difficult to fully account for or control. Considering each level of risk, including legal obligations, and promoting regular audits under the supervision of a single responsible individual within the organization can assist in identifying and mitigating the risks associated with third-party involvement. That also includes trying to ensure that the third party has the same dedication to developing cultures of security that your organization does. ▲

Notes

[1] Kelly Sheridan, "Rubrik data leak is another cloud misconfiguration horror story," Dark Reading (1/30/2019). *https://www.darkreading.com/cloud/rubrik-data-leak-is-another-cloud-misconfiguration-horror-story/d/d-id/1333767*

[2] Brian Krebs, "Target hackers broke in via HVAC company," Krebs on Security (2/14/2014). *https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/*


OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION
VOLUME LXXVII NUMBER VI
JULY 2020
www.mnbar.org
Bench&Bar
NESOTA
MSBA President 2020-21
DYAN EBERT
Steady as she goes
The big question: Back to the office?
The business interruption pandemic
Ethics wake-up calls for supervisory responsibilities
Child safety first: Reporting child abuse and neglect
Minnesota legislative session recap

Law&Technology | BY MARK LANTERMAN

Cyber riots and hacktivism

As the calendar turned to June and the nation continued to cope with the aftermath of the killing of George Floyd, the Minnesota Senate allegedly fell victim to the international hacktivist group Anonymous. On June 2, the Senate's servers were breached and passwords used by senators and staff were accessed, resulting in web pages going down. As noted in the Pioneer Press, "In a tweet, the hacking movement Anonymous highlighted the hack, which appears to have included a defacement of a Senate web page showing an Anonymous calling card and saying 'Justice for George Floyd.'"[1] While it cannot be definitively determined whether this was really an Anonymous attack, it comes in the midst of a number of distributed denial of service (DDoS) attacks against Minnesota government web pages. Even as rioting recedes in the streets of Minneapolis and throughout the nation, cyber rioting and hacktivism will continue to be of concern.

'Hacktivism' can be defined as acts of cybercrime motivated by political or social causes. Anonymous is an international, decentralized hacktivist group that is being reenergized by the recent protests.[2] Since there is no clear leader to this group, new factions can be created very quickly and work together to enact largescale attacks. The social upheaval and widespread anger washing over our world fuels this group and makes it attractive to those who want to protest and riot from a distance, "anonymously."

Threat actors tend to have financial gain as their primary motivator. Ransomware and phishing attacks are typically examples of money-driven cybercrime. Hacktivism is more personal, and the mindset of a hacker with a social or political agenda may have an impact on how an attack is conducted. Apart from the team effort that groups like Anonymous are able to marshal, hacktivist attacks may be more tenacious than your average cybercrime venture, and government entities may be particularly targeted.

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 risks of a hacktivist attack are largely operational, as is evident by the recent attacks perpetrated in Minnesota. DDoS attacks seek to make a system or network unusable for a period of time by disrupting services to users. Government websites and data will most likely continue to be threatened by hacktivist groups, in addition to law enforcement agencies. Companies and organizations with government clients or contracts and individuals related to those involved in the tragic death of George Floyd may also encounter a greater number of cyber events.

As we continue to struggle with the ongoing limitations spawned by the coronavirus pandemic and compounded by the recent events calling for social reform and justice, it is important to consider how our clients and colleagues may be affected digitally as well as in "real time." Staying apprised of best cybersecurity practices and keeping up with the current cyber landscape is important to ensuring the safety and efficiency of our digital spaces, especially as many of us continue to work remotely.

In closing, a lesson from the Minnesota Senate hacking: It is always wise to avoid having a "Passwords File." Passwords stored in text files on network-connected devices contributed to the scope and severity of this breach. Regular backup policies, VPNS, avoiding public WiFi, and the general advice to "slow down" online in an effort to reduce the risk of falling prey to phishing attacks are all simple ways to mitigate cyberthreats. ▲

[1] *https://www.twincities.com/2020/06/02/minnesota-senate-computers-hacked-passwords-file-accessed-web-pages-down/*

[2] *https://www.reuters.com/article/us-minneapolis-protests-anonymous/hackers-and-hucksters-reinvigorate-anonymous-brand-amid-protests-idUSKBN23A06I*

Compliance & Ethics Professional

April 2016

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

FEATURE

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.

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.

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: 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

FEATURE

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.

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.

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?

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?

FEATURE

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**

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVI NUMBER 1
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

Law&Technology | BY MARK LANTERMAN & JUDGE JAMES ROSENBAUM

"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.

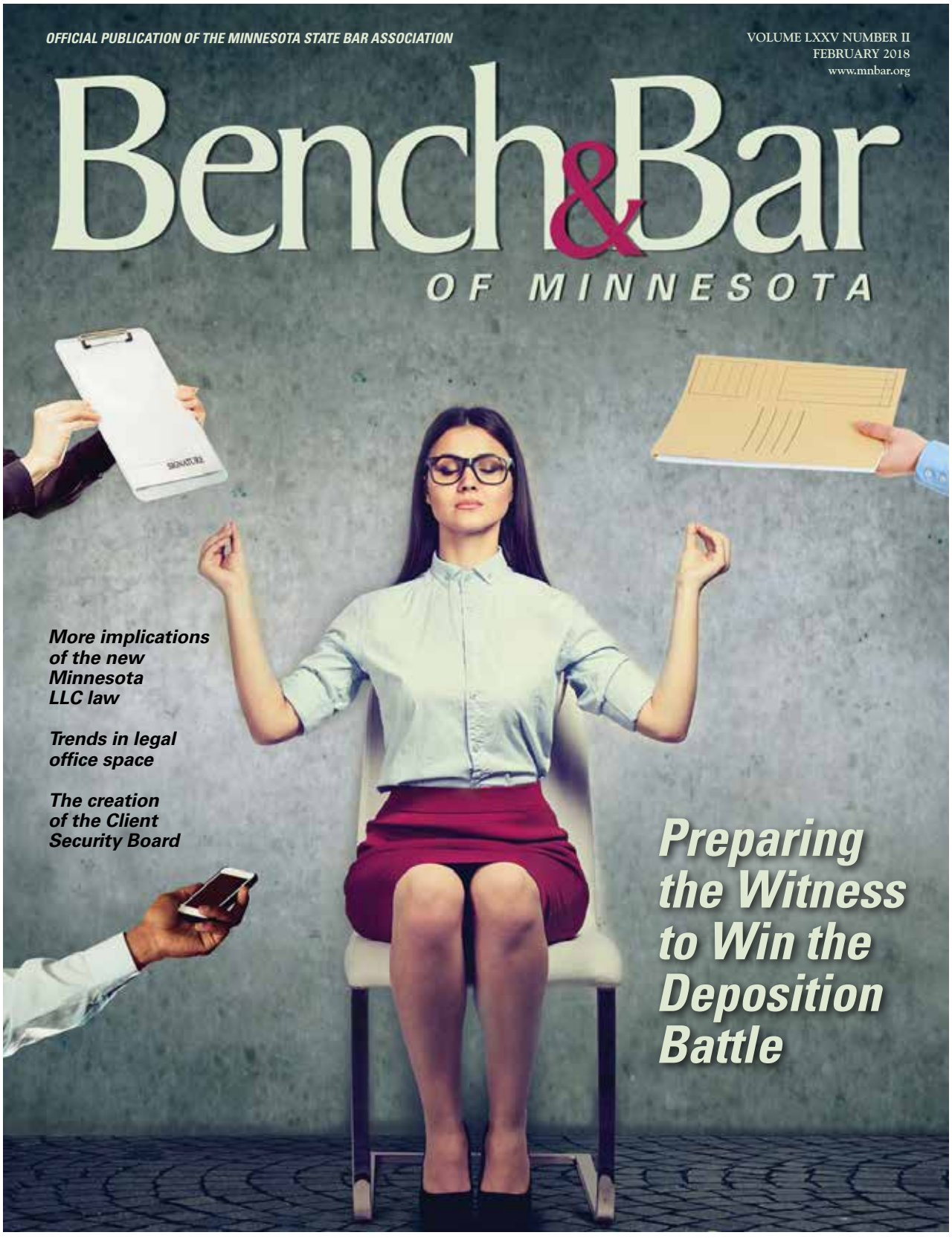
The authors of this article suggest that the courts need to refine and redefine the 4th Amendment's protection of "papers and effects" as it applies to executing a search warrant of electronic data-storing devices. If an investigator may not look into a sugar bowl to find evidence of stolen televisions, 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 LXXV NUMBER II
FEBRUARY 2018
www.mnbar.org
Bench&Bar
OF MINNESOTA
More implications of the new Minnesota LLC law
Trends in legal office space
The creation of the Client Security Board
Preparing the Witness to Win the Deposition Battle

Law&Technology

By Mark Lanterman

Is the Internet of Things spying on you?

So is your phone spying on you? Yes, it's possible.

A few months ago, Computer Forensic Services analyst Sean Lanterman spoke to KARE 11 News about a topic that makes a lot of people nervous. "Is my phone spying on me?" may have seemed like a paranoid question at one point, but it now seems like a perfectly plausible notion. Given the vast amounts of data created, stored, and transmitted by the average person's phone, it's actually a question we should all be asking. Sean pointed out the very real fact that our phones are basically snitches in our pockets, and it's not impossible that advertisers would take advantage of this fact. After all, what better source of information is there than our phones when it comes to gathering intel about our preferences, shopping trends, and habits?

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.

So is your phone spying on you? Yes, it's possible. Your smartphone's capabilities allow for the kind of spying that many suspect; your phone may communicate information about you to advertisers, and from there, personalize ads to match what has been gathered. This information can be gathered in pretty sneaky ways, too—for instance, by using your phone's microphone to capture your conversations without your awareness. The question can grow still more complicated when you apply it to your other internet-connected devices. Smartphones are probably the biggest storehouses of our personal information that we utilize on a daily basis, and for that reason, they are probably the devices that transmit the most data about us as well. But now, internet-connected devices can include everything from your thermostat to your car to your refrigerator.

These devices often feature a large range of multimedia capabilities that extend far beyond their technical use. Microphones and cameras are common elements of some of our internet-connected devices, not to mention other more advanced technologies such as GPS and voice recognition. To further confuse things, the average consumer may not know which devices have which features, especially since something as simple as a washing machine may now be equipped with exceedingly advanced technology. How do we manage all of these devices and ensure the best possible security practices?

Keeping a tally of all the internet-connected devices in your home may be more difficult than you think. Smartphones, watches, laptops, computers, entertainment systems, security cameras, TVs, cars, and the types of home appliances mentioned earlier may come to mind. But there are also trickier sources of internet-connection lurking in your home, like your kids' toys. And at the community level, everything from water plants to the power grid are connected by the internet. Can we effectively manage the risks to our privacy and security when so many of the devices we now rely on store and communicate our personal information? And what do we do when this information is compromised or our devices are taken over by cybercrime? Many of us are familiar with company and organizational policies relating to cybersecurity best practices. But when it comes to our own homes, many are less equipped and less eager to train themselves and their families in cybersecurity.

First, taking stock of which devices could potentially be spying on you, besides your phone, is important. Understanding what you buy is critical to maximizing effective use of the product and minimizing the potential risks. This is especially important when privacy concerns come into play. Knowledge of your devices includes a basic understanding of what kinds of data they collect, how this data is stored, and why and how it is communicated. If a microphone is suspected of being the culprit in leaking information, navigate settings to figure out a way to turn it off. Ideally, this kind of research is done beforehand, but proper device setup and knowledge of an item's security features can be critical in mitigating risk. Ultimately, you may decide that an internet-connected thermostat or fire detector isn't worth the hassle.

Second, once you've decided which devices are worth keeping around, take stock of the potential threats against your privacy and security. You may not be completely aware of the devices that create, save, and communicate sensitive information about you. Even though many people click the "I agree" button, most are not fully aware of what their consent implies, or means for the companies that profit from this kind of mass data sharing. A compromised device can also be used to execute greater attacks. It should be noted that hackers don't discriminate. An internet-connected device is always a target, regardless of whether it's a toy, a phone, or a computer.

If one or more devices are spying on you, it's difficult to pinpoint who or what is doing it. As Sean explained on KARE 11, there are no individuals at the receiving end, but rather an automated process comprising advanced algorithms to decipher the data being sent. Knowing how best to configure the settings on your internet-connected devices, and being aware of how many devices may pose security and privacy risks, are two keys to a proactive approach to minimizing the potential of digital spying. ▲

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXV NUMBER III
MARCH 2018
www.mnbar.org

Bench&Bar OF MINNESOTA

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

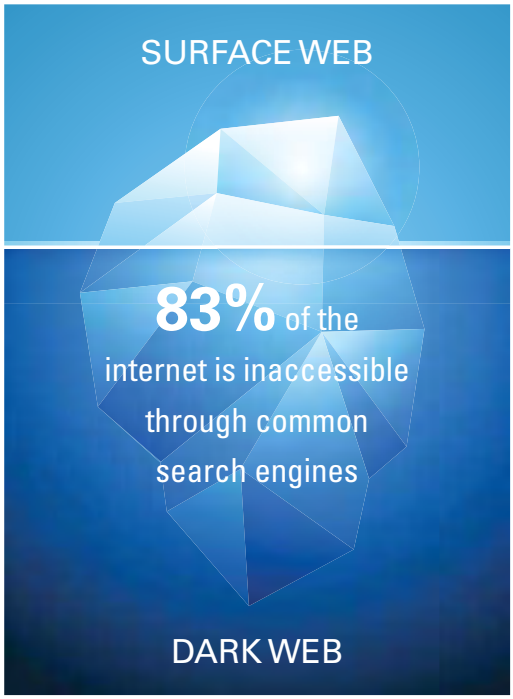
Beyond the travel ban: Headaches for employers

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.

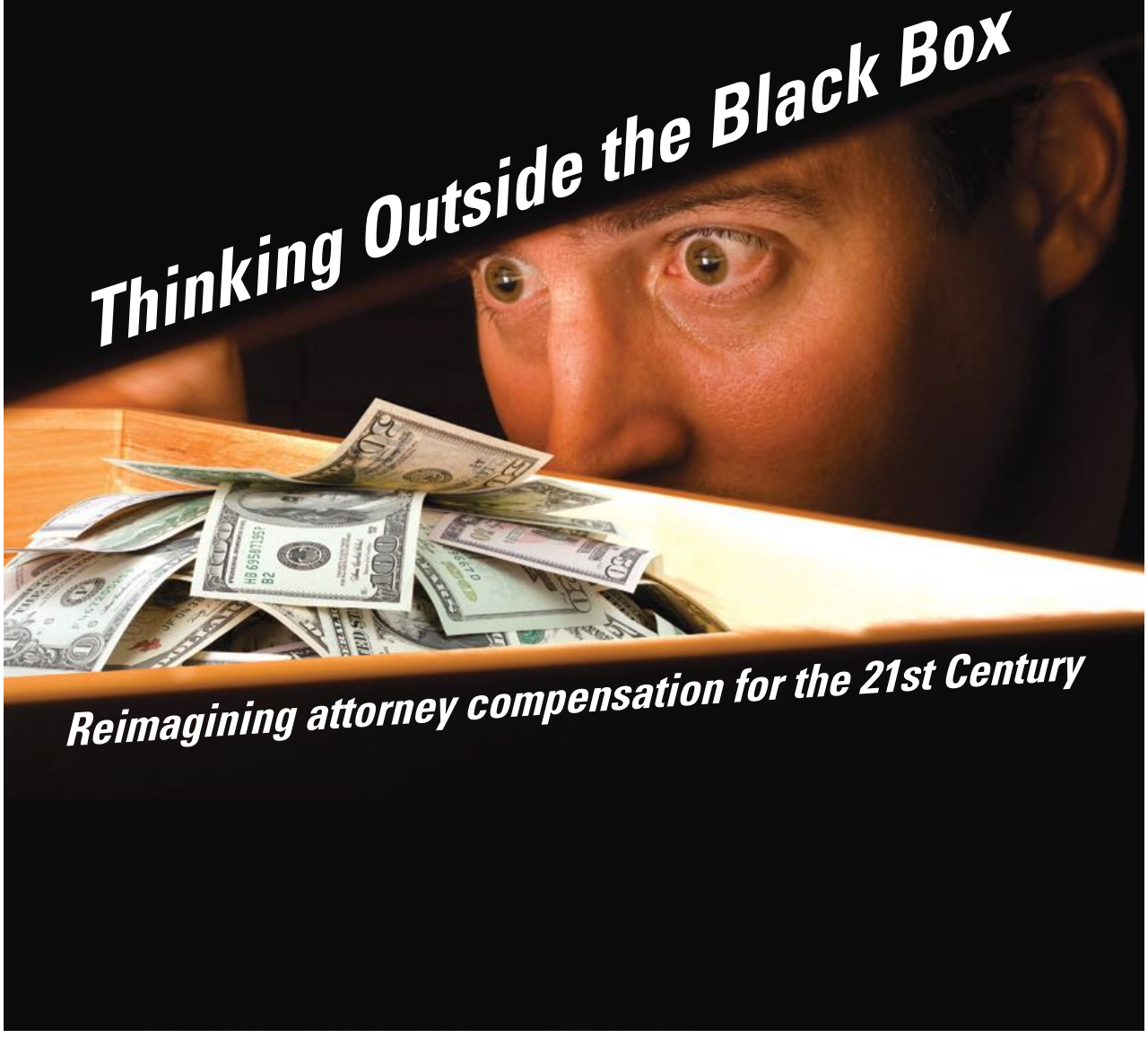
Allwine's digital narrative also revealed a browsing history consistent with his intention to murder Amy and his desire to frame fictitious parties. On more than one occasion, Allwine reviewed his and Amy's insurance policies as well as real estate and future home construction possibilities. In an effort 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

Law&Technology | BY MARK LANTERMAN

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 III
MARCH 2021
www.mnbar.org

Bench&Bar OF MINNESOTA

DEMOCRACY GOES TO COURT

Litigating voting rights and election administration

Examining high-profile complaints against election attorneys

Law&Technology | BY MARK LANTERMAN

Ransomware and federal sanctions

Ransomware, as most of us know by now, is a type of malware that takes data or devices hostage, with cyber attackers demanding the payment of a ransom in exchange for restored access. Preparation is the critical factor when it comes to handling a ransomware attack. Strong backup policies are essential for mitigating data loss; adhering to best security practices, such as the use of encryption, also better enables organizations to respond to cyber threats. While attackers may still have the ability to threaten the publication of data, it is always advisable to not pay ransoms. Paying a ransom puts an organization at greater risk of repeat attacks. But paying a ransom is also ultimately risky for another reason—it may be a violation of U.S. sanctions laws.

Given the increased reliance on remote work capabilities in 2020, ransomware attacks abounded. This added threat led the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) to issue an advisory in October detailing the additional compliance risks associated with paying ransoms. On a national level, "ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States."[1] Even if the identity of the attacker is unknown, a victim may still commit a violation if they pay a ransom to a sanctioned individual or entity. Furthermore, individuals who assist or facilitate payments on behalf of a victim—including attorneys, insurance companies, and security vendors—may also be at risk of sanctions violations.

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.

Individuals who assist or facilitate payments on behalf of a victim—including attorneys, insurance companies, and security vendors—may also be at risk of sanctions violations.

When confronted with a ransomware attack, organizations become panicked and want the incident to be resolved at any cost. Many of them rush to pay the cyber terrorist. The risk of losing access to data can be preventively managed with a strong data backup policy, along with the implementation of strong information security controls. In some instances, organizations may still feel the need to pay cyber attackers in the hope that doing so will prevent publication of their data. But paying the ransom does not guarantee that the attacker will actually do what they say; it remains a possibility that the data will be posted or sold regardless of whether the victim pays. Paying ransoms fuels cyberterrorism internationally and puts the victim, and others, at greater risk.

OFAC guidelines

While the penalties for violating sanctions laws are steep and contribute to the legal, reputational, financial, and operational risks that accompany ransomware attacks, OFAC provides guidelines for appropriate response procedures and ways to potentially mitigate the repercussions of inadvertently committing a violation. If a violation is identified, "the existence, nature, and adequacy of a sanctions compliance program is a factor that OFAC may consider when determining an appropriate enforcement response."[2] A Framework for OFAC Compliance Commitments has been published to assist organizations in creating this type of program.[3] Having this in place reduces the risk of a violation to begin with, and potentially improves the outcome in the event of a violation. The five key categories identified by OFAC as primary components of a risk-based program are similar to the necessary factors contributing to a strong security culture. Proper response procedures at the time of an attack also reflect favorably on an organization, including contacting OFAC and appropriate law enforcement agencies.

In assessing the potential risks associated with ransomware, it is important to consider the possibility of violating sanctions laws. Cyberattacks often come with a web of risks; preparation and adherence to best practices help to offset the uncertainty. Developing a strong compliance culture and establishing a strong incident response plan are important to proactively address risk. ▲

Notes

[1] *https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf*
[2] *https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf*
[3] *https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf*


OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION
VOLUME LXXVI NUMBER IV
APRIL2019
www.mnbar.org
Bench&Bar
OF MINNESOTA
9 ways to fail as an entrepreneur
You can't serve two masters. Unless you're a Realtor.
A tribal counsel's guide to corporate compliance
Understanding tortious interference with contract
Minnesota Parentage Law and Assisted Reproductive Technology
It's time to change the law

Law&Technology | BY MARK LANTERMAN

Security considerations for law firm data governance

The legal community deals with a huge amount of data. Legal strategies, client communications, research, e-discovery, documentation, billing, personal information about clients—the list of data types with which law firms are entrusted every day is continuously growing. Effective data management is critical, as immediate access to data is just as important as keeping it protected. Data governance frameworks assist in keeping in compliance with current regulations and standards.

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.

Data governance refers to a framework establishing how the data that an organization collects and stores should be managed, accessed, and kept private. How this framework is structured largely depends on the types of data being collected, and it also assigns responsibilities for invested stakeholders who are held accountable for certain elements of the management process. Because law firms need to manage an array of complicated data, delegation is critical. Data management should not be solely the concern of the IT department. Upper management support and involvement helps set expectations for data governance, especially with regard to budgeting and the allocation of necessary resources.

Laying out this degree of communication within a firm about its data governance strategy requires data stewardship. Data stewards are assigned to specific data assets or business processes and take particular responsibility for how it is accessed and protected.

More is not better

Data governance strategies should specify how long certain types of data are to be retained and how and when it is destroyed. Storing large amounts of inactive data (especially confidential or personally identifying information) makes law firms a prime target for breaches. Data architecture frameworks are used to document what data assets are being stored and where, as well as their movement within the network. Data inventories should be consistently updated to make data minimization easier to organize and execute.

Data frameworks are critical in clearly communicating within the firm what types of data are being amassed, where it is being stored, and what technologies should be used to manage it, such as cloud infrastructures. Cloud computing allows for immediate access to data from internet-enabled devices without the physical storing of data within an organization's immediate proximity or location. Remote servers enable employees to access data from anywhere. The cloud is a cost-effective and simpler technology for many organizations, and replaces centralized data storing with a distributed and expanded framework. That said, this decentralized system requires a strong relationship with your provider, an understanding of what data is being stored, who your client is, and what amount of risk you are willing to take. Implementing cloud security solutions is important for dealing with data that is not completely in your control. Encryption policies and user education also balance data protection with immediate accessibility.

Strongest possible controls

Law firms are being pushed to implement the strongest possible information governance controls and procedures. Clients have high expectations for data security, and recent international laws draw attention to an increase in future cybersecurity pressures within the United States. The General Data Protection Regulation (GDPR) has a significant impact on U.S.-based law firms that have clients with protected EU status. Breach notification, consent for how data is collected and used, data minimization, and breach assessments are all elements of what is required by the GDPR. "All customer-facing documentation will require revision to comply with the GDPR," notes a recent article in the magazine

American Gaming Lawyer, "which requires providing detailed information to data subjects regarding the processing of personal data in a concise, transparent, intelligible, and easily accessible form." Strong data governance frameworks make compliance with security regulations feasible.

The reputational, financial, and legal risks associated with a data breach impacting a law firm are severe. Huge stores of data, increased utilization of the Internet of Things, and varied mobile devices, cyber regulations, and client expectations for data privacy all make for a very complicated set of requirements by which law firms have to abide. Data governance frameworks assign accountability and promote interdepartmental communication, upper level support of secure data policies, and the use of tech tools and resources to protect and access data. Preparing for data breaches with strong incident response plans that take into account compliance (and the costs associated with non-compliance), having qualified security personnel, and perhaps investing in cyber insurance all help to demonstrate to clients a firm's focus on keeping their data secure. ▲


OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION
VOLUME LXXVIII NUMBER IV
APRIL 2021
www.mnbar.org
Bench&Bar
OF MINNESOTA
Competent but compromised
Representing clients on the spectrum between mental health and mental illness

Law&Technology | BY MARK LANTERMAN

Geofence warrants
The battle is just beginning

This past February, a TechCrunch article explained how geofence warrants were being used to identify those involved in the Minneapolis protests of last summer. With a judge's approval, geofence warrants essentially allow law enforcement to obtain information on anyone who was in a particular area at a particular time. With these general perimeters, it is more than possible that individuals who are not involved in any criminal activity will have their information requested simply for matching the search criteria. The article describes how one Minneapolis resident, Said Abduallahi, "received an email from Google stating that his account information was subject to the warrant, and would be given to the police. But Abdullahi said he had no part in the violence and was only in the area to video the protests."[1]

Geofence warrants mark a clear divide between those who prioritize privacy and those who want to use the long arm of surveillance technology for law enforcement. For law enforcement, geofence warrants are a powerful tool in identifying offenders; in addition to the Minneapolis protests, these warrants were widely used to locate rioters involved in the January 6 U.S. Capitol insurrection. As the Washington Post noted afterward, "The Capitol, more than most buildings, has a vast cellular and wireless data infrastructure… Such infrastructure, such as individual cell towers, can turn any connected phone into its own tracking device."[2] Historically, Google cooperates with law enforcement in providing anonymized user data, following up with more specific information for potential suspects; in fact, these sorts of warrants saw a 500 percent request increase between 2018 and 2019.[3] While this degree of connectivity provides law enforcement with an easy tracking method, many argue that the risks and potential abuses of this capability outweigh the benefits.

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.

By their nature, these warrants can have serious impacts upon the guilty and innocent alike. Given this impartiality, it is frequently argued that the tool facilitates unconstitutional searches and seizures. Those who are caught up in the net are often surprised to learn the extent of the geographical data that has been collected about them—and with their permission! User agreements, such as those with Google, make information sharing under certain circumstances permissible. With that in mind, it is most likely that geofence warrants and the associated concerns with their use will be addressed by the courts; the first major case to confront the potential Fourth Amendment violations of geofence warrants involves a 2019 armed robbery that occurred in Virginia.[4] In Illinois, U.S. Magistrate Judge Gabriel Fuentes rejected a warrant request involving a drug theft case, stating, "if the government can identify that wrongdoer only by sifting through the identities of unknown innocent persons… a federal court in the United States of America should not permit the intrusion."[5] But in the meantime, these warrants will most likely continue to be used extensively by law enforcement.

In using the multitude of applications on our smart phones, we often fail to recognize the vast amounts of personal data that we allow to be collected, stored, and in some instances, shared with other parties. It is always important to be mindful of our technological footprint and the policies employed by major organizations such as Apple or Google. Since most of us tend to click "agree" without a thought, it is also wise to research and understand how your data is being used. Google now deletes location history data after 18 months, and Apple has stated with respect to providing product backdoors and broad government access, "We believe security shouldn't come at the expense of individual privacy."[6] But Apple also complies with legally valid requests. Unfortunately there are no perfect methods to control and monitor the huge volume of data we allow to be collected about us. ▲

Notes

1 *https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant/*
2 *https://www.washingtonpost.com/technology/2021/01/08/trump-mob-tech-arrests/*
3 *https://www.abajournal.com/magazine/article/law-enforcement-is-using-location-tracking-on-mobile-devices-to-identify-suspects-geofence*
4 *https://www.nacdl.org/Content/United-States-v-Chatrie,-No-3-19-cr-130-(E-D-Va-)*
5 *https://www.abajournal.com/magazine/article/law-enforcement-is-using-location-tracking-on-mobile-devices-to-identify-suspects-geofence*
6 *https://www.apple.com/privacy/government-information-requests/*


OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION
VOLUME LXXIV NUMBER V
MAY/JUNE 2017
www.mnbar.org
Bench&Bar
OF MINNESOTA
GRAVE MATTERS
The law and practice of disinterment, reinterment, and exhumation in Minnesota
WE'RE MOVING!
Why You May Need an LLC Update
Your Personal Data – Or Is It?
An Out of Court Article on Hearsay
RENEW YOUR MSBA DUES AT: MNBAR.ORG/RENEW

Your Personal Data – Or Is It?

Doxxing and online information resellers pose threats to the legal community

By Mark Lanterman

Photo © iStockphoto

Given the sensitive nature of the courtroom and of the emotions that may arise there, attorneys, judges, and others in the legal community are at particular risk of becoming victims of doxxing-related crime. *Doxxing* is a term used to describe the buying, selling, gathering, posting, or distributing of private information online. Importantly, doxxing is typically carried out with malicious intent and is often aimed at damaging someone's reputation. As opposed to the mere gathering of information from someone's Facebook or LinkedIn profile, doxxing is often abetted by targeted data breaches. The distinction here is that anyone who posts on social media is essentially allowing the public at large to view, and use, that information. The kinds of private information spread through doxxing are not typically shared by the subjects themselves.

Everything from health to legal information is valuable to cybercriminals and hackers, and it is therefore exactly the kind of information that is commonly put on online. Apart from financial data, information related to health and legal circumstances can be of particular interest to an individual interested in harming another's reputation or career. Unfortunately, many doxxing victims don't realize that they have become victims until something serious has occurred or they realize that the information has already been widely distributed.

Though the personal information-gathering associated with doxxing can often be assisted by cyberattacks, doxxing itself is not necessarily illegal. Many people are not aware that their private information is widely available on personal information reseller websites. These websites are easily accessible by the average user, no Dark Web required. The information contained on these sites can divulge where you live, who your past employers were, and can even connect you to the last person living in your home or apartment. Fortunately, these websites give people the ability to opt out and remove their information. The problem is that the actual time it takes to remove the info, or the processes required to achieve this, can be confusing or cumbersome depending on the website.

Furthermore, some of the websites do not directly store your private information, but rather give users a list of other websites that do. For this reason, the individual is left to chase down their information on a number of websites instead of just one. And the fact is, even if someone takes the time to opt out of each one of these websites, it is very possible that they will repopulate their sites within a matter of months with the same information you requested be taken down. With this in mind, I would say that the majority of people are not aware of exactly how much private information is available about them online at any given time.

Private information can be used to physically stalk, harass, or threaten individuals. But it can also be used to harm a person's reputation or disrupt the victim's personal life. Recent headlines have focused on judges that have been targeted; however, everyone in the legal community is at an increasing risk of having their private information accessed without consent or knowledge. Given the rise of the Internet of Things (IoT), more and more data from our daily lives is being collected, stored, and distributed. Though this may be convenient, more data makes for a greater risk that it will be compromised. The number of devices comprising the IoT also makes for a wider array of potential access points for the cybercriminal. Since the process of doxxing often relies on the successful execution of data breaches, the Internet of Things presents the perfect blend of vulnerabilities and useful data.

The legal community is not immune to the changes brought about by the IoT. Living in a world of interconnected devices makes for easier communication, more efficient workflows, simpler data collection and storage, and a generally

OPT-OUT FORMS FOR MAJOR PERSONAL INFO RESELLERS

LINKS	VERIFICATION NEEDED	TURN-AROUND TIME
pipl.com/help/remove	Pipl is a search engine that does not host personal information, but it is a good starting point for identifying personal information from other sources.	Depends on other sources from which Pipl populates its search results.
www.beenverified.com/optout	Email address	24 hours in most cases
www.checkpeople.com/optout	None	7-14 days
www.intelius.com/optout.php	Government-issued ID	7-14 days
www.peoplesmart.com/optout-go	Email address	Up to 72 hours
www.publicrecords360.com/optout.html	State-issued ID	This site does not disclose turn-around time.
www.spokeo.com/opt_out/new	Email address	30 minutes
support.whitepages.com	Email address and phone number	Immediate
www.zabasearch.com/block_records	Redacted state-issued ID card or driver's license	4-6 weeks
www.zoominfo.com/lookupEmail	Email address	"Within a few days"
www.familytreenow.com/optout	Email address	Unknown

more productive way of managing things. Smartphones and Wi-Fi-connected devices mean greater accessibility and use of our personal information; for many IT departments, this convenience is the most important consideration when developing new technology policies. But the IoT is as risky as it is convenient. Many people don't understand the sheer amount of data that is being produced and stored about them. And each connected device is essentially another access point for a cybercriminal to compromise this data. For the same reasons that connectivity is great for communication, it is detrimental for security and keeping vulnerabilities contained.

In addition to providing opt-out information in this article, I will also provide some realistic risk-management advice. While it often feels as if the expansion of our digital lives is necessary, taking stock of the risks is important in managing security. For those in the legal community, developing a sound cybersecurity protocol is not only a responsibility to clients. It is also an important step in protecting your own privacy and keeping your personal information safe.

When assessing your current cybersecurity strategies, try to look from the outside in. Identify what data is most important and valuable. Also try to figure out where this data is currently being kept and what measures are in place to safeguard it against cyberattacks. Issues of employee compliance or outdated policies may arise during this examination, but making this kind of assessment is a very important step toward improvement.

To help those who are interested, I'm listing the names of several major personal information resellers and corresponding information about how to remove your personal data from their websites.

Opting out of personal information reseller websites is a solid step toward bettering your online behaviors. Keeping private information secure is not automatically guaranteed, especially when there are websites that profit from selling your info to anyone who might be interested. And like other cybersecurity protocols, checking these kinds of websites should be done fairly regularly. Opting out only removes the information that is currently posted; it doesn't necessarily prevent one of these websites from re-populating with your personal information in the future. Also, bear in mind that it is important to be proactive when it comes to removing your information the first time. Be mindful of the websites' turn-around times and don't let your opt-out request fall of your radar, or theirs, in the meantime. Though it may seem like an annoying chore, for those that are worried about becoming victims of doxxing, it is well worth the effort.

Like many changes that have arisen with the Internet of Things, doxxing is yet another issue that may affect you. Being mindful of what data you are sharing through your digital devices and doing your best to monitor your online presence are important elements of your personal cybersecurity strategy. Protecting your personal information is ultimately just as important as protecting your clients' data. ▲

***MARK LANTERMAN** is the 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. Mark has 28 years of security and forensic experience and has testified in over 2000 cases. He is an adjunct instructor for the University of Minnesota M.Sci. Security and Technology program, Mitchell Hamline Law School, and the National Judicial College in Reno, Nevada. Mark also conducts training for the Federal Judicial Center in Washington, D.C.*
MLANTERMAN@COMPFORENSICS.COM

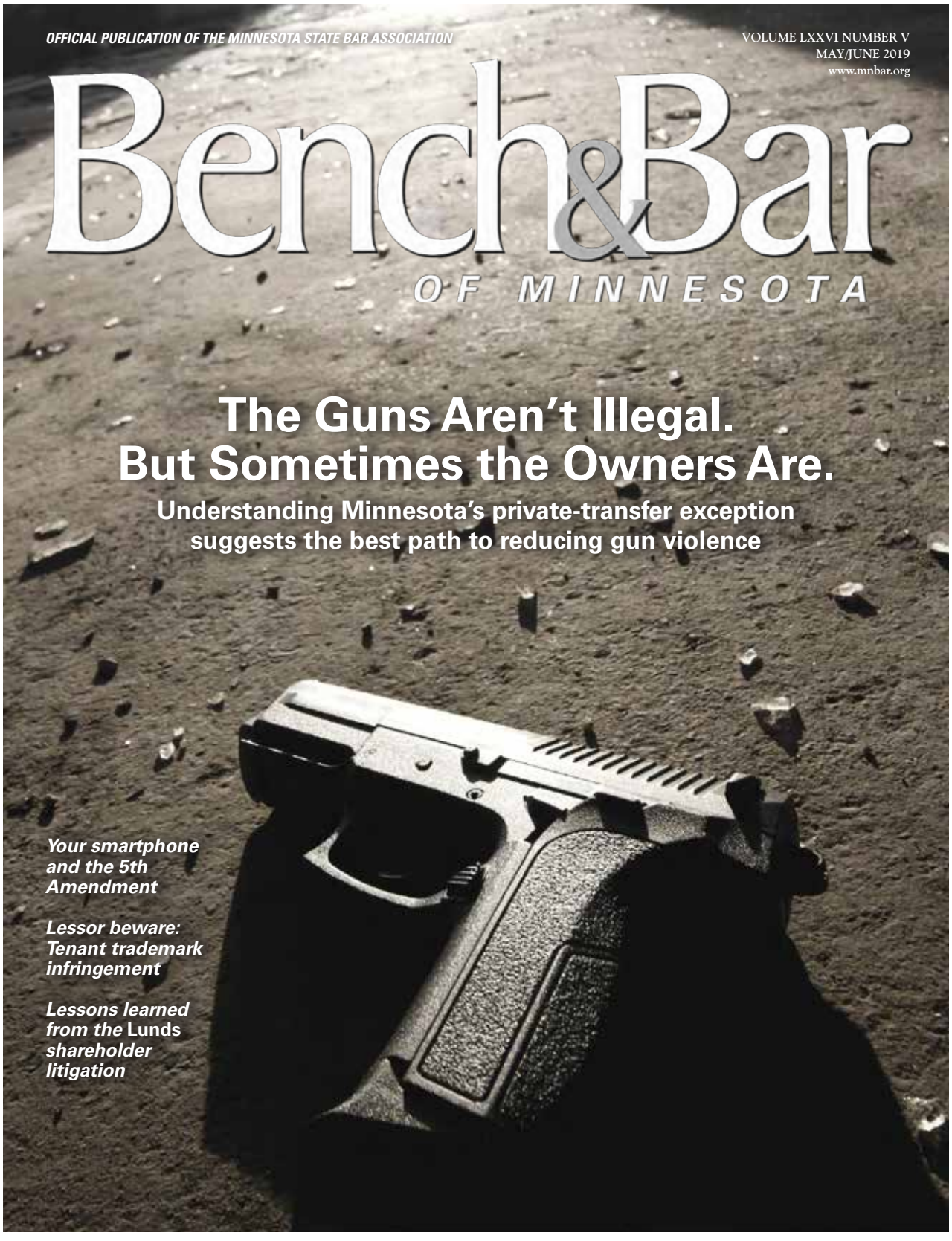
OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

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*

Law&Technology | BY MARK LANTERMAN & JUDGE JAMES ROSENBAUM

"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.

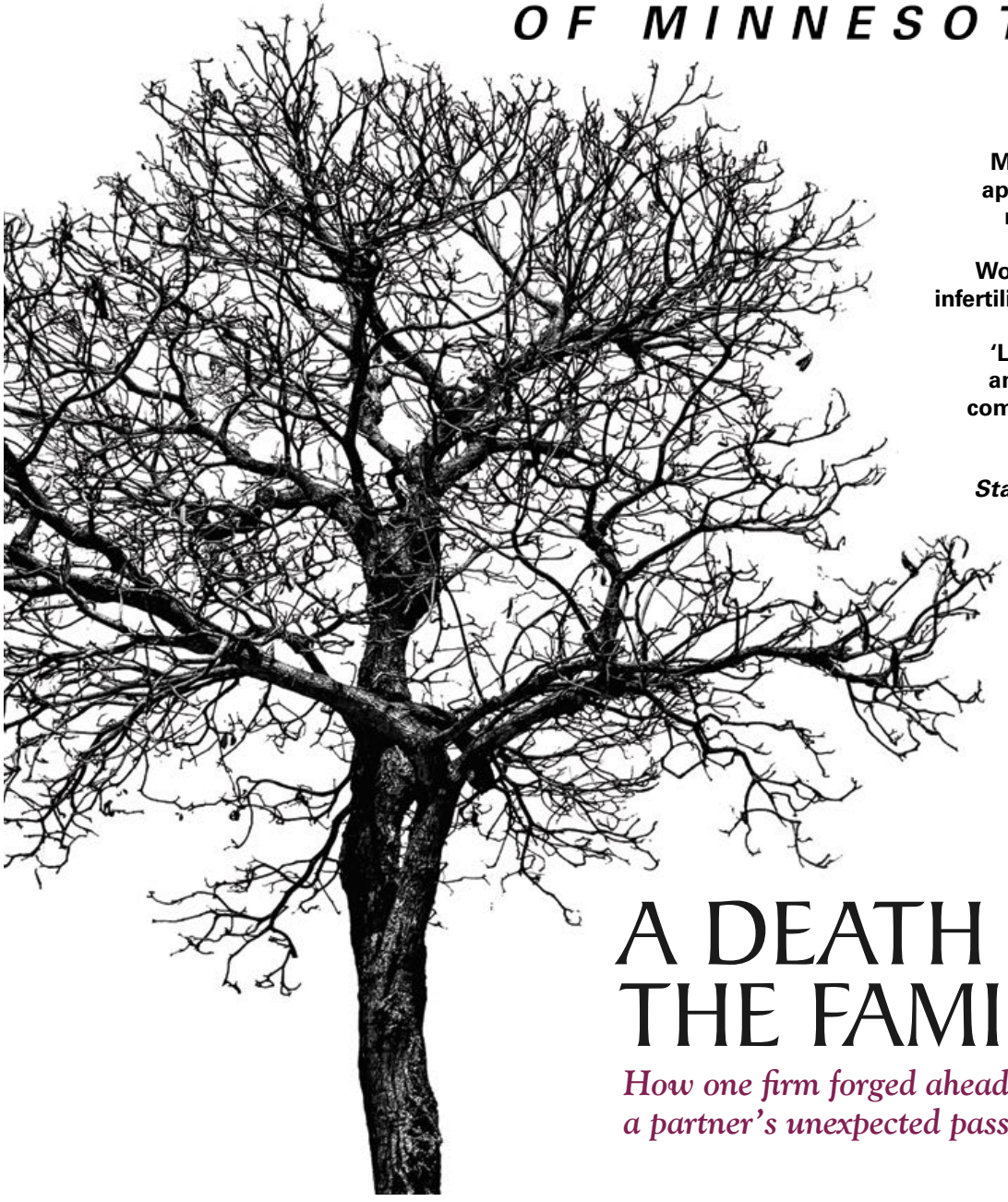
The law is properly recognizing that our digital world requires a new level of warrant specificity. For the majority of Americans, these devices contain private details about almost every, if not every, aspect of our lives. The fact that technology now enables an individual to carry such information 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 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

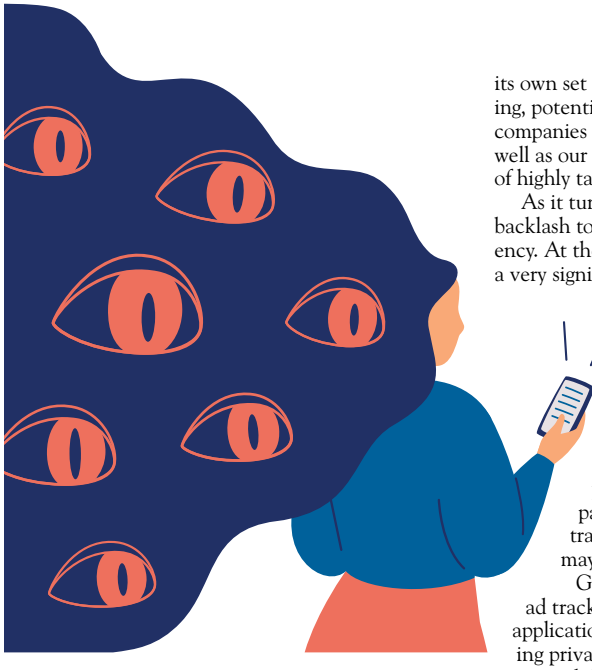
Media got *State v. Khalil* all wrong

A DEATH IN THE FAMILY

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

Law&Technology | BY MARK LANTERMAN

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

Law&Technology | BY MARK LANTERMAN

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 LXXVI NUMBER VI
JULY 2019
www.mnbar.org
Bench&Bar
MINNESOTA
MSBA President 2019-20
TOM NELSON
A Life of Service
Proving moral change in reinstatement and bar admission cases
The case for mandatory legal malpractice insurance
U.S. Supreme Court protects trademark licensees

Physical security should be part of your incident response plan

In their efforts to assure the best and strongest cybersecurity measures, I think many organizations need to get back to basics. To effectively mitigate the risks associated with the cyberthreats we face every day (phishing, malware, social engineering, tailgating, etc.), organizations rely on cybersecurity measures to protect their critical networks, systems, and data. But they also rely on physical security measures as a critical protection against intrusion. The goal of physical security is to prevent "hands-on" tampering, theft, or destruction of critical technologies, information systems, or data. If a criminal walks into your office and steals a box full of important client data, this constitutes a breach as surely as if it had happened over your networks.

Physical security is too often seen as a category separate from cybersecurity, even though they both share the same objectives. A holistic approach to security requires that both of these areas be combined in organizational cyber policies, procedures, and incident response plans. Just as an organization should have practiced, well-documented measures in place for responding to a data breach, it should be well known what the procedure is for handling physical breaches of security.

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 CIA triad

Information security is guided by the terms set forth in the CIA triad model: "In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people." This model is used to help direct and articulate the tenets of an ideal information security program. Physical security aims to prevent disruption to organizational physical assets—especially assets relating to information systems—without limiting their operationality. These measures prevent misuse, damage, unauthorized access, and unauthorized removal from the primary physical location.

Establishing physical security baselines requires a consistently updated and reviewed log of assets, as well as a mobile device management (MDM) solution that manages and tracks all portable devices. Other methods of physical security include barriers to personnel-only areas, card keys that limit access to information technology to relevant personnel (such as IT departments and upper management), and various detection devices. More sophisticated measures may also include behavior detection to actively seek out potential attackers, depending on the size of the organization and the assets in need of protection.

Keep in mind that physical security issues are similar to cyber threats in that while your organization is trying to bar potential outsiders, it may be the insider threat that ultimately causes the damage. If a disgruntled employee gains access to the server room and inserts a thumb drive infected with malware, that is a breach of physical security as well as cybersecurity. Social engineering attacks can also be conducted in physical space and may facilitate unauthorized access. Limiting access controls is critical both in physical and cyberspace. Preventing "access creep" requires vigilance and frequent review, especially when employees are terminated.

A question of mindset

In addition to established, centralized access control and identity management when it comes to authorizing employees to access information systems, integrating physical security and cybersecurity practices must entail a comprehensive and visible implementation method. This includes understanding that cybersecurity is a company-wide initiative that extends far beyond the IT department as well as using physical security to support these practices; thus, everyone needs to participate in ensuring the protection of systems, networks, and data. On the level of personnel, access controls are better managed with a combined approach (especially when a new employee is hired). As the Internet of Things allows remote access that extends far beyond the physical space of the office, security measures must take identity management into account. The physical security of third-party vendors should also be audited regularly.

Combining physical security and cybersecurity protocols is important. Physical security is often treated separately or overlooked altogether in creating an organization's cyber posture; it deserves to be viewed as a foundational part of any security plan. Keeping track of, and improving upon, physical security measures should be part of standard security assessments. They can even be used to demonstrate to employees how easy it may be to enact social engineering attacks by taking advantage of physical vulnerabilities. Experts agree that holistic approaches to security are always stronger than a segmented protocol. Viewing physical security as an administrative responsibility and prioritizing cybersecurity measures leaves an organization vulnerable to myriad easily preventable attacks and intrusions. ▲


OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION
VOLUME LXXVII NUMBER VI
JULY 2020
www.mnbar.org
Bench&Bar
NESOTA
MSBA President 2020-21
DYAN EBERT
Steady as she goes
The big question: Back to the office?
The business interruption pandemic
Ethics wake-up calls for supervisory responsibilities
Child safety first: Reporting child abuse and neglect
Minnesota legislative session recap

Law&Technology | BY MARK LANTERMAN

Cyber riots and hacktivism

As the calendar turned to June and the nation continued to cope with the aftermath of the killing of George Floyd, the Minnesota Senate allegedly fell victim to the international hacktivist group Anonymous. On June 2, the Senate's servers were breached and passwords used by senators and staff were accessed, resulting in web pages going down. As noted in the Pioneer Press, "In a tweet, the hacking movement Anonymous highlighted the hack, which appears to have included a defacement of a Senate web page showing an Anonymous calling card and saying 'Justice for George Floyd.'"[1] While it cannot be definitively determined whether this was really an Anonymous attack, it comes in the midst of a number of distributed denial of service (DDoS) attacks against Minnesota government web pages. Even as rioting recedes in the streets of Minneapolis and throughout the nation, cyber rioting and hacktivism will continue to be of concern.

'Hacktivism' can be defined as acts of cybercrime motivated by political or social causes. Anonymous is an international, decentralized hacktivist group that is being reenergized by the recent protests.[2] Since there is no clear leader to this group, new factions can be created very quickly and work together to enact largescale attacks. The social upheaval and widespread anger washing over our world fuels this group and makes it attractive to those who want to protest and riot from a distance, "anonymously."

Threat actors tend to have financial gain as their primary motivator. Ransomware and phishing attacks are typically examples of money-driven cybercrime. Hacktivism is more personal, and the mindset of a hacker with a social or political agenda may have an impact on how an attack is conducted. Apart from the team effort that groups like Anonymous are able to marshal, hacktivist attacks may be more tenacious than your average cybercrime venture, and government entities may be particularly targeted.

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.

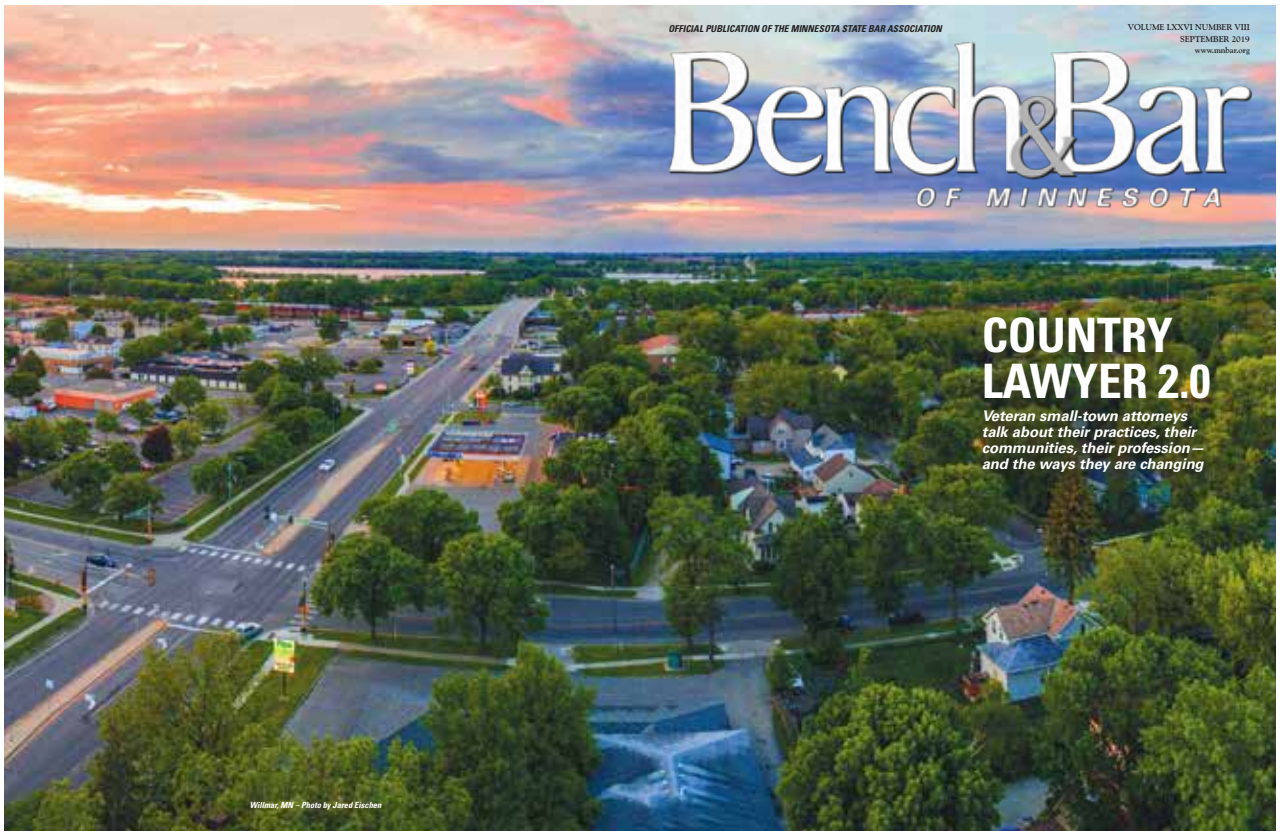
The risks of a hacktivist attack are largely operational, as is evident by the recent attacks perpetrated in Minnesota. DDoS attacks seek to make a system or network unusable for a period of time by disrupting services to users. Government websites and data will most likely continue to be threatened by hacktivist groups, in addition to law enforcement agencies. Companies and organizations with government clients or contracts and individuals related to those involved in the tragic death of George Floyd may also encounter a greater number of cyber events.

As we continue to struggle with the ongoing limitations spawned by the coronavirus pandemic and compounded by the recent events calling for social reform and justice, it is important to consider how our clients and colleagues may be affected digitally as well as in "real time." Staying apprised of best cybersecurity practices and keeping up with the current cyber landscape is important to ensuring the safety and efficiency of our digital spaces, especially as many of us continue to work remotely.

In closing, a lesson from the Minnesota Senate hacking: It is always wise to avoid having a "Passwords File." Passwords stored in text files on network-connected devices contributed to the scope and severity of this breach. Regular backup policies, VPNS, avoiding public WiFi, and the general advice to "slow down" online in an effort to reduce the risk of falling prey to phishing attacks are all simple ways to mitigate cyberthreats. ▲

[1] *https://www.twincities.com/2020/06/02/minnesota-senate-computers-hacked-passwords-file-accessed-web-pages-down/*

[2] *https://www.reuters.com/article/us-minneapolis-protests-anonymous/hackers-and-hucksters-reinvigorate-anonymous-brand-amid-protests-idUSKBN23A06I*


OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION
VOLUME LXXVI NUMBER VIII
SEPTEMBER 2019
www.mnbar.org
Bench&Bar
OF MINNESOTA
COUNTRY LAWYER 2.0
Veteran small-town attorneys talk about their practices, their communities, their profession—and the ways they are changing
Willmar, MN – Photo by Jared Eischen

Law&Technology | BY MARK LANTERMAN

Too secure? Encryption and law enforcement

The U.S. government is reviving a push to force technology companies to undermine their own security by creating backdoors for the sake of easier law enforcement access. This past July, Attorney General William Barr revived the anti-encryption fight that most of us have probably already heard during a speech at the International Conference on Cyber Security at Fordham University. The main idea, as set forth by Barr, is the primary argument that's been put forth previously: "While encryption protects against cyberattacks, deploying it in warrant-proof form jeopardizes public safety more generally. The net effect is to reduce the overall security of society." Since criminals often use encryption to hide their activities from law enforcement, in other words, law enforcement should be granted a backdoor into the safeguards that keep the average user optimally secure from cybercrime.

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.

Just as in response to the San Bernardino terrorist shooting, in which Apple's security was targeted in order to gain access to a suspect's phone, tech companies are having to defend their pursuit of optimal security. One of these methods is an increasing use of encryption for consumers who want the best in data protection. Though Barr insists that law enforcement access must be made possible by weakening encryption, security experts agree that any purposefully created security vulnerability is a vulnerability that anyone may be able to exploit. No matter how skillfully implemented, it would remain entirely possible—if not likely—that it would only be a matter of time until unauthorized individuals or entities take advantage.

Encryption provides a valuable layer of security within organizations and for individual users by making data unreadable unless accessed with the correct key. Organizations rely on encryption to best protect client data. Without encryption, confidential data would be more readily available to cybercriminals.

Broad implications

More personally, the implications of weakened encryption for the average user are far-reaching. For the sake of making criminal investigations allegedly easier for law enforcement to conduct, each and every individual who uses encryption to better secure their data would be more at risk of compromise. Easier law enforcement access would create easier access for all, including foreign governments.

The law enforcement community has needed to adjust to the ever-changing and expanding network of challenges posed by technology. The smartphones most people carry in their pockets contain huge amounts of information pertaining to our daily lives, not to mention the stores of information contained on our other devices. These devices are huge potential sources of evidence for law enforcement, and it is absolutely true that immense hurdles often need to be overcome in order to access them effectively, if at all. It is also often true that critical information pertaining to a case may only be gathered through accessing a device.

Drawing the line

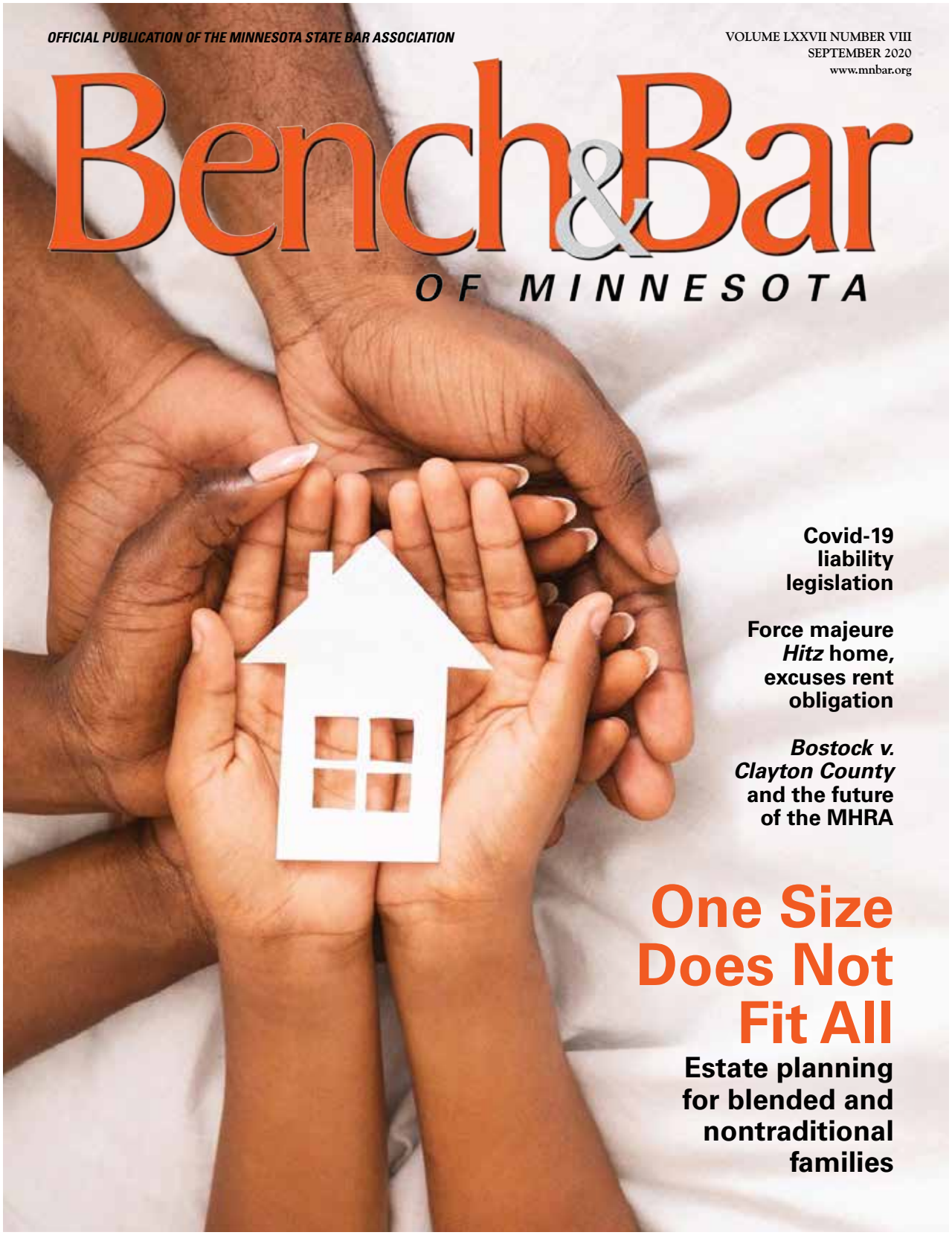
But weakening everyone's security cannot be an antidote for stymied criminal investigations. Technology companies are yet again being placed in a position where they have to defend the security of their devices—albeit, in this case, for being too secure. The burden must ultimately be placed on law enforcement to get creative when it comes to accessing digital devices. The way the majority of people bank, access health information, pay bills, and store their personal information cannot be purposefully compromised. Dangerous repercussions would result from forcing large organizations to use weakened encryption (or none at all). It is in everyone's best interest that the data stored on our devices be kept as secure as possible.

Barr believes that "making our virtual world more secure should not come at the expense of making us more vulnerable in the real world." What he fails to realize is that without digital security, we cannot have "real world" security. Our digital spaces are entirely intertwined with our real world. Technology certainly can be used for malicious or terroristic purposes. That is, unfortunately, a reality of our society that cannot be denied. But strengthening cybersecurity is going to assist the vast majority in protecting themselves against crime while continuing to take advantage of the vast array of benefits that technology offers. ▲

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

Law&Technology | BY MARK LANTERMAN

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*


OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION
VOLUME LXXIV NUMBER IX
OCTOBER 2017
www.mnbar.org
Bench&Bar
OF MINNESOTA
How "trial lawyer" became an oxymoron
No time? No problem! Two great online pro bono outlets
Facial recognition technology brings security & privacy concerns
Inspired to Serve
In-house pro bono is on the rise

Law&Technology

By Mark Lanterman

Facial recognition technology brings security & privacy concerns

In recent years, facial recognition technology has had some great successes. They include recognizing the faces involved in terroristic attacks, scanning faces at the airport for identification instead of using a passport, and—now—becoming a feature of our digital devices. It's clear that new applications of this technology are being utilized to streamline and simplify.

Facial recognition is a biometric identifier, but it has very different implications from using our fingerprints, or more traditionally, our passcodes. While some point to their similarities, it is very important to recognize that biometrical markers are not necessarily interchangeable, depending on their application.

FRT as biometrical authentication

Not all human characteristics are created equal when it comes to being used as biometrical markers. Eye scans, fingerprints, and facial recognition are probably the most prevalent, though all have weaknesses, strengths, and associated risks. Even among this group, each has different applications that vary widely depending on the environment in which they are being used. Some are more expensive than others, more difficult to use, or come with varying degrees of accuracy. While eye scans are typically very expensive and require a lengthy enrollment process, and fingerprints cannot be used for surveillance purposes, facial recognition technology theoretically enables identification from a distance and doesn't require as much work getting individuals enrolled.

MARK LANTERMAN is the chief technology officer of Computer Forensic Services. A former member of the U. S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security and forensic experience and has testified in over 2,000 cases.

Some key variables surrounding biometrical markers involve the kind and degree of protection these identifiers are afforded in court. Recent cases include a verdict allowing an individual to be forced to give her fingerprint to unlock a phone. This situation sparked a debate over what an individual "has" (their fingerprint) vs. what he or she "knows" (their passcode) and whether there's a difference when both serve the same purpose. Since smartphones are essentially snitches we carry around in our pockets and typically contain huge amounts of information, it is not surprising that "what" is being unlocked with a biometrical marker is a very important consideration.

It was ultimately determined that a fingerprint is different in kind from a passcode, because it's classified as something that someone has. But what will the ruling be when it's someone's face and they may or may not be aware that it's being used to unlock a device or to surveil them without their knowledge? Clearly, issues of privacy and security will be at the forefront, as people attempt to determine a balance between convenience, privacy, and security.

Surveillance, privacy, and security

Facial recognition technology poses a number of interesting problems because it implies a degree of surveillance of which the average person may not be aware. Should people have to consent? How will this information be stored once collected? Will the uses of this information be transparent? When using a biometrical marker that is—unlike a fingerprint—readily perceptible, it is important to consider how people will be informed of how this identifier is to be used, and what the benefits are on a wider scale.

Clearly, privacy is also at stake when using facial recognition technology. Compared to using a fingerprint as the go-to method of opening your phone, using your face may be even more problematic. The September 12 Apple Keynote described the newest iPhone, iPhone X, and one of its most amazing features: Face ID. By using the improved camera, Face ID serves as the new authentication for opening an iPhone. While the security aspects seem strong—there is a purported 1 in 1,000,000 chance that a stranger will be able to open your phone with his or her face—it's important to remember the implications of biometrical authentication for law enforcement. Since your face is something you have, not something you know, it's also important to recognize that this biometric marker is most likely not going to have the same protections as a passcode in court. Given that this feature is always "on" and can be used in almost any condition, night or day, it's clear that it would be fairly easy for law enforcement to obtain access to someone's phone.

Using your face as your digital identifier also comes with security risks. If someone gets your biometric information, there is seemingly little that can be done, especially since facial information is more or less unchangeable. And unfortunately, many experts agree that facial recognition technology is currently not as accurate as fingerprint technology, meaning it may be easier to access a phone with a faulty scan. Or a photo stolen from a social media account. Keeping a passcode safe is one thing, but especially today, many people post a number of photos of themselves that may be the key to anything using facial recognition technology. While Apple assured its customers that Face ID is secure, it should be acknowledged that what may be secure today will not necessarily be secure tomorrow.

In sum, facial recognition technology poses the same kind of problem as many other technologies that make our lives easier. Where convenience is gained, privacy and security are often diminished. While we may be assured today by security efforts, that may change: Cybercriminals tend to adapt quickly to new technologies and new vulnerabilities. And while facial recognition technology may be easier to use than a passcode, it comes with the same privacy caveats as any other biometrical identifier in court. ▲

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVI NUMBER IX
OCTOBER 2019
www.mnbar.org

Bench&Bar OF MINNESOTA

Litigating Harassment in the #MeToo Era

A lingering gap between the letter of the law and the mood of the culture is yielding strikingly disparate outcomes in sexual harassment cases

AI and its impact on law firm cybersecurity

The rise of artificial intelligence has a number of implications within the legal community. Apart from its impact on operational tasks and its potential for increasing efficiency, AI will likely feature as an element of in-house cybersecurity policies and practices.

Efforts to counteract cyber threats are becoming as sophisticated as the technologies we use on a daily basis. Law firms are especially at risk of cybercrime due to the sensitive information they create and store. Personally identifying information, data relating to litigation, and client communications are only some of the data types a typical law firm will store and access on a daily basis. This data make law firms prime targets for a variety of threat actors, especially when paired with less-than-ideal security standards. In the face of ever-expanding threats, many organizations are turning to artificial intelligence to assist in their cybersecurity initiatives. At a time when budgeting for security is often not seen as a priority, it is significant that almost half of enterprises surveyed in a recent study by the Capgemini Research Institute (*Reinventing Cybersecurity with Artificial Intelligence*) say that their budgets for cybersecurity AI will increase by an average of 29 percent in Fiscal Year 2020.[1]

As organizations grow and embrace new technologies, their risk of data breaches and cyber events increases. More employees, more devices, and trends toward BYOD (bring your own device) policies, cloud infrastructures, and remote work all make for potential sources of vulnerability. The Internet of Things also creates a much wider zone in which cybercriminals can act. With this pattern in mind, organizations have to consider what the best course of action will be when, not if, they are attacked. Law firms use these technologies too, often managing them with convenience and ease of use as the top priorities.

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.

Focusing on detection

As set forth in the Capgemini study, at this point enterprises are largely turning to AI solutions for the purposes of detection. As cyber events come to seem increasingly inevitable, organizations are facing the fact that early detection may be the best course of action. The sooner a cyber event is detected, the sooner it can be mitigated. Speedy mitigation helps organizations keep the costs associated with breaches as low as possible by ensuring that threat actors have less time to exploit vulnerabilities and exfiltrate data.

But as AI is implemented over time, it will also be beneficial in creating proactive solutions, both predictive and responsive.[2] These methods will undoubtedly spur new policies as organizations learn to use AI to its fullest potential.

It remains to be seen how AI will be incorporated into each facet of a cybersecurity policy, but it will most likely continue to be an instrumental component of a strong security program for its reactive and proactive potential. Reduced attack times make for a reduction in the financial, operational, and reputational risks that organizations face from cyber events. Its implementation may also evolve into a requirement of cyber insurance policies, along with regularly scheduled risk assessments.

The human element

With IT professionals increasingly overburdened, the use of AI to bolster security efforts helps to minimize human error. But the human component can never be completely removed. False positives and issues brought about by insufficient data will still need to be monitored and assessed by security professionals. In spite of its myriad benefits, especially within settings where confidential data is at stake, AI will never be a foolproof safety net. The complexities of developing security cultures, creating proactive strategies, and navigating the intricacies of public response and mitigation strategies are still issues that will require human attention.

Early detection, network intrusion scanning, email attack surveillance, and user behavior analysis are just some of the ways that AI is being used to strengthen security.[3] Given this multitude of functions, many experts believe that AI will also be put to use by cybercriminals, with large-scale cyberattack campaigns a primary concern. As these issues materialize, they will require the expertise of security professionals to create sustainable solutions. The defensive capabilities of AI will be needed to counteract the ways in which it can be utilized aggressively by bad actors. This technology poses yet another instance of organizations and security professionals alike needing to balance security with convenience, and ease of use with the acknowledgement that no security measure is ever going to be a "cure-all."

The legal community is undoubtedly tasked with maintaining the highest of standards in regard to protecting client data. As AI continues to shape the ways in which law firms conduct business, it is critical to stay apprised of its equally important role in reinforcing security postures. ▲

Notes

[1] *https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/#1322c0a4117e*

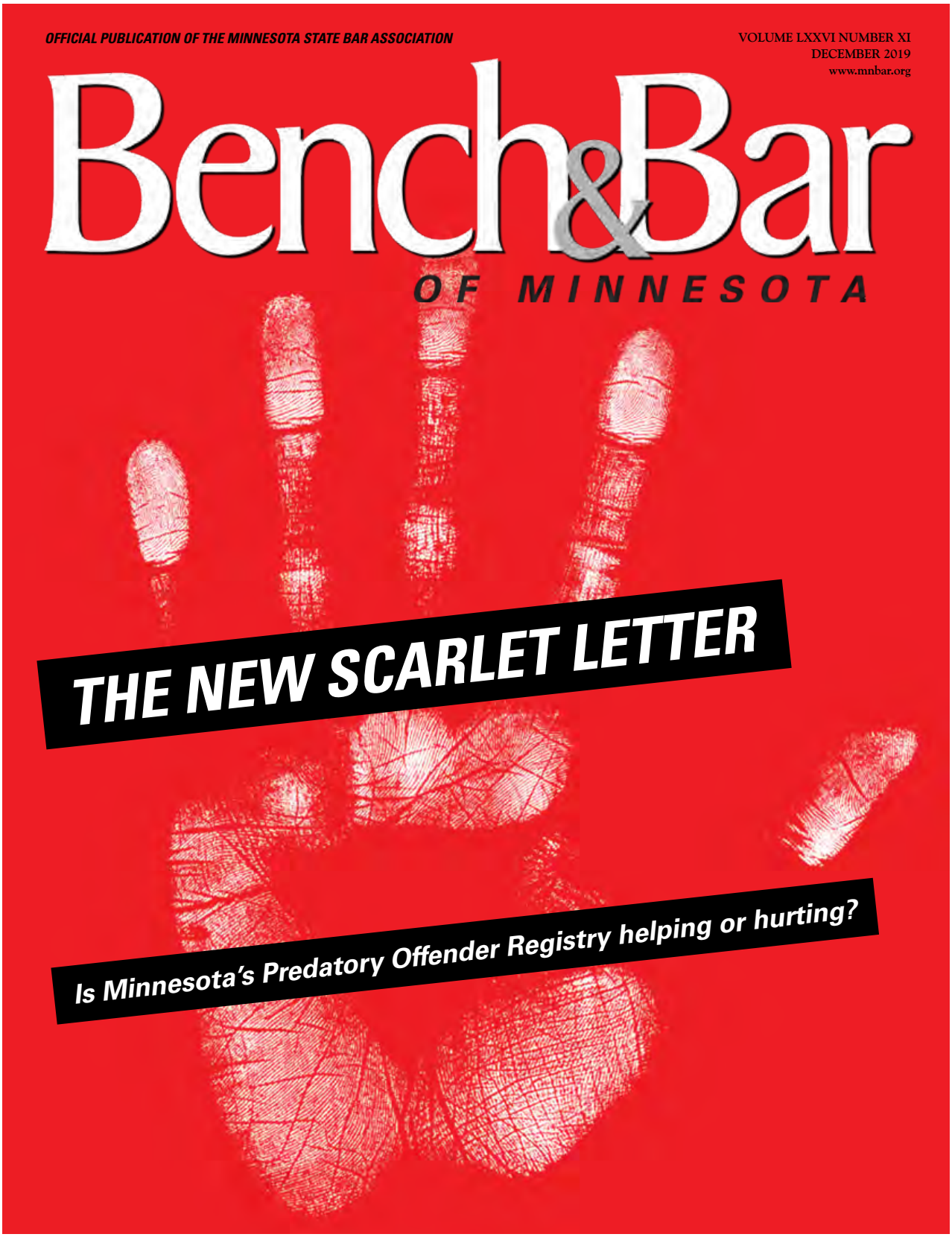
[2] *Id.*

[3] *https://resources.infosecinstitute.com/ai-in-cybersecurity/#gref*

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVI NUMBER XI
DECEMBER 2019
www.mnbar.org

Bench&Bar OF MINNESOTA



THE NEW SCARLET LETTER

Is Minnesota's Predatory Offender Registry helping or hurting?

Law&Technology | BY MARK LANTERMAN

Doxxing redux: The trouble with opting out

Back in the spring of 2017, I wrote an article on doxxing and the types of reseller websites that often make it possible ("Your personal data – or is it?" May/June 2017). Doxxing is generally understood as the buying, selling, gathering, or other sharing of personal information online, often with malicious intent. With this private information in hand, individuals can threaten, stalk, harass, or damage the reputations of others. Members of the legal community are at particular risk of having their information accessed and used without their knowledge or direct consent.

As I described in my first article on the topic, personally identifiable information (PII) reseller websites make obtaining this information pretty easy. By visiting one of numerous sites, a person can find a wide range of private information that includes an individual's address, phone number, criminal history, and employment situation, not to mention a slew of details about their spouse (past or present), children, and family members.

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.

I think most people would be surprised to learn the full scope of what's lurking about them on the web. In response to the risks, people are often encouraged to complete opt-out requests through these sites. I have previously provided a short listing. The problem with opting out? Well, there's more than one.

First, the sheer number of these sites makes it difficult if not impossible to fully monitor your personal information. It's one thing to continuously opt out of one, two, or three PII reseller websites. It's another thing entirely to pursue removing your information from a dozen or more sites, only to have new sites of which you're unaware pop up within a month. And if the information you're concerned about isn't on one of these sites, it could very well be available elsewhere.

Second, these websites typically make it as difficult as possible to remove your information. There are opt-out pages (the links to which frequently change) for many of these sites. But they often require lots of additional information from the user to remove their details. For example, the website Public Records 360 "will only process opt out requests received by online submission, or fax, and no request will be processed without complete information (i.e., name, address and date of birth)." Official identification such as a driver's license or passport is typically required; otherwise someone can send a notarized identification verification form.[1] Providing this information also poses a security risk, and users are often left wondering if it's worth the additional hassle and uncertainty.

Third, while some of these sites mention their turn-around time for removing your information once a request has been sent, others do not. In addition to monitoring a number of sites—the number of which changes continually as new sites are brought to our attention—users also have to follow up to make sure the requests that they have made are being honored. If a site doesn't give a turn-around time, users will have to continuously check up on whether their information has actually been taken down from the site. These issues are only a small fraction of the larger problems that arise in trying to control your online presence.

While PII reseller websites are important culprits in disseminating the types of information that make doxxing possible, it is also important to remember the variety of data brokers to whom we routinely hand over private information. Earlier this year, Vermont passed the country's first law seeking to manage "data brokers," those companies that routinely collect and store our info. According to the Office of the Vermont Attorney General, "The new law requires Data Brokers to register with the Secretary of State annually and maintain certain minimum data security standards."[2] The law requires that data breaches be reported, that certain data security standards be enacted, and that opt-out information be provided if applicable.[3] The types of data brokers that this law affects include websites like Spokeo, but they also include a wide range of larger and smaller data gatherers.

While securing compliance with laws like Vermont's may prove difficult in the long term, the growing pressure for their passage certainly highlights growing consumer demand for transparency and control of PII. Hopefully, a growing body of legislation will assist with the lack of clarity that characterizes the buying, selling, and availability of our data online. ▲

Notes

[1] *https://www.publicrecords360.com/optout.html*

[2] *https://ago.vermont.gov/blog/2018/12/13/attorney-generals-office-issues-guidance-on-data-broker-regulations/*

[3] *https://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf*

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**

Faculty

Mark Lanterman is the chief technology officer of Computer Forensic Services in Hopkins, Minn. Before entering the private sector, he was a member of the U.S. Secret Service Electronic Crimes Taskforce. Mr. Lanterman has 28 years of security and forensic experience and has testified in more than 2,000 cases. He also is faculty for the Federal Judicial Center in Washington, D.C., the National Judicial College in Reno, Nev., the University of Minnesota and the Mitchell Hamline Law School. In additoion, he is a professor in the cybersecurity program at the St. Thomas School of Law in Minneapolis. Mr. Lanterman has provided training in digital evidence, computer forensics and cyber security to the U.S. Supreme Court. He has also presented to the Eighth and Eleventh Circuit Federal Judicial Conferences, as well as numerous state and federal Judicial Conferences across the U.S. He is a member of the Minnesota Lawyers Professional Responsibility Board and chairs its Opinions Committee. Mr. Lanterman completed his postgraduate studies in cybersecurity at Harvard University and is certified as a Seized Computer Evidence Recovery Specialist (SCERS) by the Department of Homeland Security.

Jon J. Lieberman is a partner at Sottile & Barile LLC in Cincinnati and has represented consumer debtors, commercial debtors, large and small creditors, mortgage lenders and servicers, automobile creditors and student loan creditors, as well as chapter 7 and 13 trustees. He has worked for some of the largest creditor firms in the region and is licensed to practice in Ohio, Kentucky, Indiana, Michigan, Colorado, Wisconsin and the District of Columbia. He is also able to practice in front of the Sixth Circuit Court of Appeals, the U.S. Court of International Trade and the U.S. Supreme Court. Mr. Lieberman served as co-chair of ABI's Consumer Bankruptcy and Legislation Committees, and he is currently Special Projects Leader of ABI's Commercial and Regulatory Law Committee. He also is an associate editor of the *ABI Journal*, co-chair of Outreach for ABI's Veterans and Servicemembers Affairs Task Force, former member of ABI's "40 Under 40" Steering Committee, and currently serves on the advisory board of ABI's Consumer Practice Extravaganza. He was selected as ABI's 2000 Committee Person of the Year, and he co-authored ABI's Thorny Issues in Consumer Bankruptcy Cases, Second Edition. Mr. Lieberman received his J.D. from the University of Cincinnati College of Law in 1990.