Easiest Catch: Don't Be Another Fish in the Dark 'Net - Cybersecurity Tips for Your Company

Mark Lanterman
Computer Forensic Services
Minnetonka

Minnesota CLE's Copyright Policy

Minnesota Continuing Legal Education wants practitioners to make the best use of these written materials but must also protect its copyright. If you wish to copy and use our CLE materials, you must first obtain permission from Minnesota CLE. Call us at 800-759-8840 or 651-227-8266 for more information. If you have any questions about our policy or want permission to make copies, do not hesitate to contact Minnesota CLE.

All authorized copies must reflect Minnesota CLE's notice of copyright.

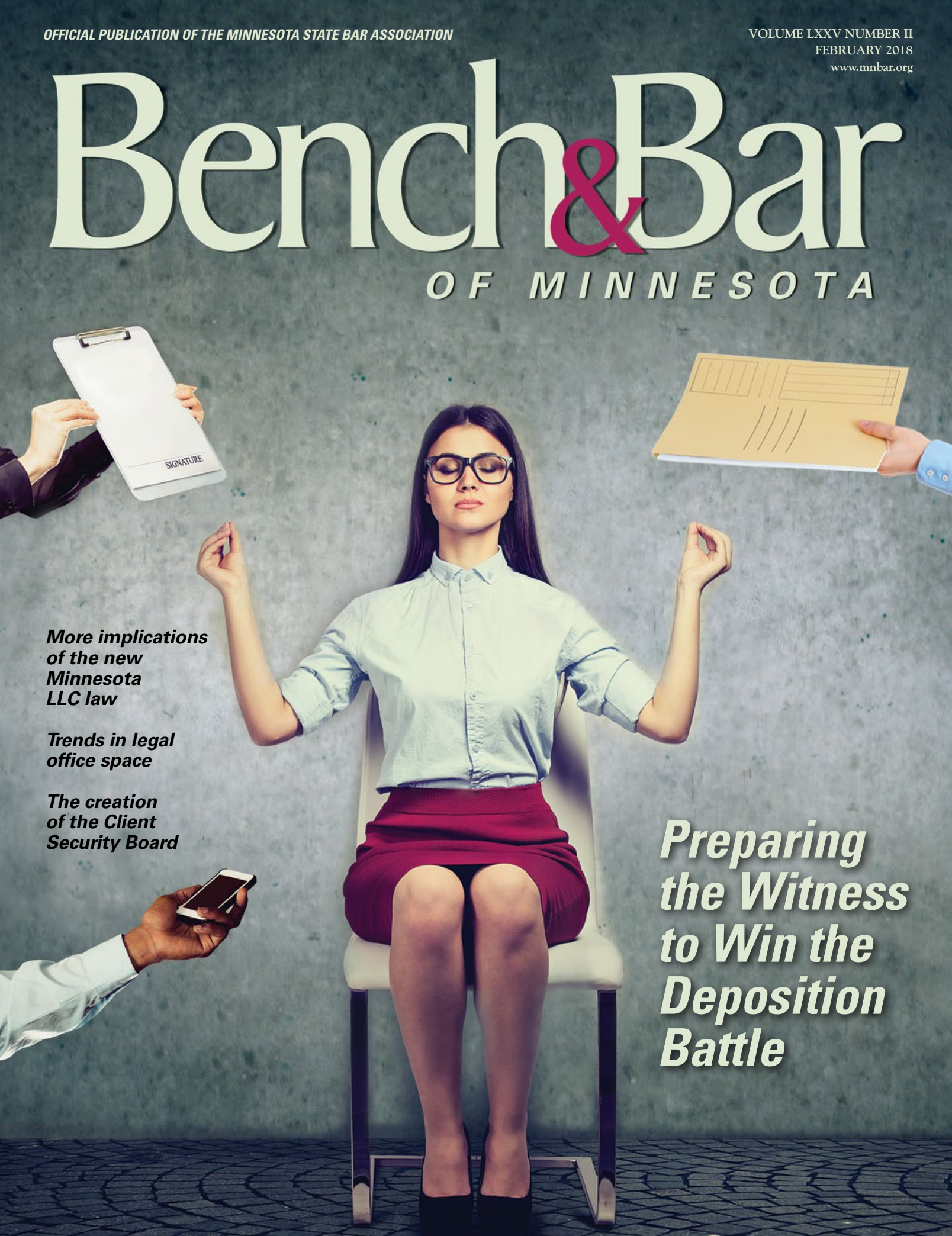
MINNESOTA CLE is Self-Supporting

A not for profit 501(c)3 corporation, Minnesota CLE is entirely self-supporting. It receives no subsidy from State Bar dues or from any other source. The only source of support is revenue from enrollment fees that registrants pay to attend Minnesota CLE programs and from amounts paid for Minnesota CLE books, supplements and digital products.

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

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

#MeToo IN THE LAW FIRM

Lessons for lawyers from the post-Weinstein reckoning

#MeToo as a moment opportunity

How to change firm culture

Trump Year One: A conversation with immigration lawyers

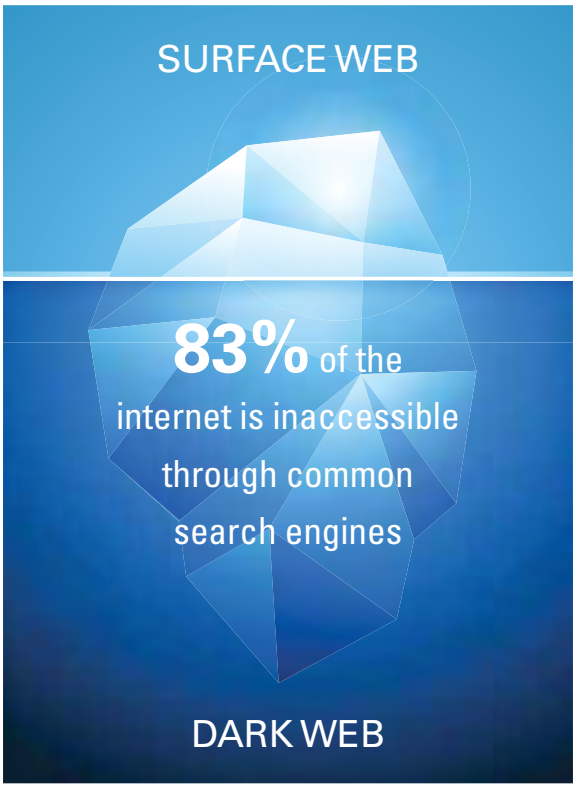
Beyond the travel ban: Headaches for employers

Stephen Allwine:

When crime tries to cover its digital tracks

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

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



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

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

Exploring the Dark Web

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

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

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

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

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

A pattern of deception

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

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

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

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXIV NUMBER X
NOVEMBER 2017
www.mnbar.org

Bench&Bar OF MINNESOTA

How Law Firms Can Prepare for Partner Retirement

Succession Planning for Small Law Firm Owners

Is your firm complying with the Minnesota Professional Firms Act?

2017 CLIO Legal Trends Report

GOODBYE TO ALL THAT

Thoughts on turning 67 and knowing when to quit

By Mark Lanterman

How digital evidence supported gerrymandering claims

Earlier this month, I had the once-in-a-lifetime opportunity to travel to the United States Supreme Court to witness the headline-making gerrymandering oral arguments out of Wisconsin. Some people are calling this case the most important of the year, with enormous potential consequences for political redistricting and any number of similar cases in which gerrymandering claims play a part.

During a five-month period in the Senate in 2012, the Democratic party made the most of its short-lived majority to gather digital evidence in support of their extreme gerrymandering claims against the Republicans. I was asked on behalf of the Campaign Legal Center in Washington, D.C. to provide digital forensic analysis of hard drives that had been gathered from Wisconsin lawmakers. These hard drives had been used by the mapping drafters and ultimately showed that one party had worked to gain a clear advantage, even in the event that they did not win a majority of votes. My analysis led to the discovery of several key deleted files, including deleted spreadsheets, that revealed a systematic pattern of intent: The metadata revealed that with each draft of the spreadsheets, the map-drawing lawmakers attempted to strengthen their party's majority and retain control.

Does delete mean deleted?

Upon my initial review of the hard drives provided, it became clear that a large number of files had been deleted immediately before the digital evidence had been delivered to my office. It is interesting to note that even at the state Senate level, key players in this case didn't understand that delete doesn't always mean deleted. I determined (and later testified) that hundreds of thousands of files had been deleted using a commercial wiping program in the week prior to the computers being turned over to Wisconsin Senator Mark Miller.

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.

The Campaign Legal Center's request for an independent forensic investigation was instrumental in constructing this case. Seeing that fraud or some kind of misconduct had most likely taken place, the court granted the request, which ultimately led to my review of the hard drives in question. The pattern of purposeful wiping further confirmed suspicions.

A second review of the digital evidence

After the first case settled out of court in 2013, I was approached again to conduct another limited analysis of the hard drives to uncover more relevant digital evidence. As attorneys built their case for the United States Supreme Court, digital evidence continued to play a key role in unraveling a narrative of purposeful, extreme gerrymandering on the part of one of the political parties.

This subsequent analysis of the provided hard drives led to the uncovering of several deleted spreadsheets, and detailed the redistricting map drafters' plans to gain a 54-45 projected majority over the other political party, regardless of whether or not they actually won the majority of votes. One particularly damning spreadsheet, labeled "Tale of the Tape," demonstrated that the minority political party in Wisconsin would need at least 54 percent of the vote to gain an Assembly majority. Clearly, the map drafters had been attempting to manipulate the mapping as much as possible to put the minority at an extreme, and perhaps unconstitutional, disadvantage.

My subsequent examination of the digital evidence also revealed some critical metadata, data which may have been overlooked had the plaintiffs opted for a simple e-discovery procedure over digital forensics. Metadata is a term used to describe "data about data," and in this instance, the critical metadata consisted of timestamps. The creation dates of the maps located on the hard drives, and their associated revisions, allowed for the reconstruction of a timeline revealing that with each round of revisions, the maps' drafters were purposefully solidifying their majority. It should be noted that these maps would determine which political party would be in control for a span of over 10 years. The stakes were high, and as with many forensic analyses, the devil was in the details.

Conclusions

The opportunity to play a role in a Supreme Court case was an amazing experience, and it served to underscore some of the things I know to be true about digital evidence. The faster you can gather it and preserve it, the better. The plaintiffs made the absolute most of their temporary majority in the Senate. Prioritizing the collection and preservation of digital evidence was a strategic move that showcased the profound impact of digital evidence in shaping the course of a case. In this instance, it could have nationwide consequences for gerrymandering and political mapping. Apart from the political consequences, I think this is a clear-cut example of how digital evidence can make a case by serving as an impartial witness in court. As if that weren't enough, I also sat directly behind Arnold Schwarzenegger during the arguments. ▲

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

Why You May Need an LLC Update

Your Personal Data – Or Is It?

An Out of Court Article on Hearsay

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 LXXIV NUMBER VII
AUGUST 2017
www.mnbar.org

Bench&Bar OF MINNESOTA

LITIGATING SPORTS CONCUSSIONS

WHAT YOU NEED TO KNOW ABOUT THE SCIENCE AND THE LAW

Ethical Considerations in Working with Aging Clients

Happy Birthday, Whistleblowers: Minnesota law turns 30

Plus

Are Title Company Kickbacks Harming Your Clients?

By Mark Lanterman

Digital evidence: New authentication standards coming

As it is now written, Federal Rule of Evidence 902 pertains to self-authenticating records such as newspapers and public records that require no external evidence to be made admissible at trial. Soon, the rule will encompass digital records generated by electronic processes in addition to records preserved directly from electronic devices or files, such as emails. This December, new amendments to Rule 902 will affect the standards for the admissibility of digital evidence. Newly proposed paragraphs 13 and 14 of Rule 902 will remove authentication hurdles for electronic evidence, whether it consists of an electronic document, file, or raw data. The proposed text of rule is as follows (emphasis added):

> The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:
>
> ***
>
> (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).

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.

With this change, digital evidence, and the story it tells, have many foundational questions out of the way. Without knowing how courts will apply the rule, however, I think that there is one caveat that will impact litigants—chain-of-custody/acceptable collection practices. With these upcoming changes in mind, it is clear that proper evidence collection and acknowledgment of best practices are critical. In this article, I will describe issues pertaining to proper digital evidence handling and the increased need for digital forensic professionals in light of these upcoming amendments.

A focus on best practices

The rules being implemented this December will greatly ease the burden of authenticating digital evidence and allow for a more cohesive system of evidence collection. These amendments largely serve to replace live testimony from any number of witnesses for the purpose of authentication with an affidavit from a certified person who can reliably attest to the evidence's authenticity. These new amendments underscore the court's increasing reliance on expert witnesses in preserving and bringing forth digital evidence.

Digital evidence is undeniably a prominent feature in the courtroom. In a growing number of situations, pieces of electronically stored information are the basis of investigations within organizations, for law enforcement, and in litigation. This degree of importance requires an equally high degree of care. Issues of authentication and proper evidence handling are particularly pertinent, since digital evidence is extremely susceptible to alteration and mishandling if not done properly by a qualified individual.

To illustrate, I will describe a typical, though always frustrating, situation that I encounter when assisting an organization or company responding to an incident involving digital evidence. Let's start here: Your company has a summer internship program. Each summer, one or two interns join your team and are assigned a number of different tasks that require varying degrees of access to your company's data. At some point during the internship period, it is discovered that one of these interns has been attempting to send confidential client data to a personal email address without prior authorization. IT is subsequently alerted and they are asked to handle the situation. Their first step is to retrieve the systems issued by the company to the offending party.

In an effort to deduce what exactly has occurred (i.e. what kinds of information were shared, with whom, and how many times), the IT person logs into the system with the intern's user credentials one day after the incident has been reported. The IT person clicks around on the intern's issued computer, trying to figure out what has transpired. This is not best practice. Although it is well-meaning, simply turning on a computer or electronic device permanently alters the state of the data. Think of it like a crime scene. Just as law enforcement wouldn't want to go snooping through a scene without taking proper precautions to ensure evidence will not be contaminated, digital evidence requires the same degree of care.

In reality, the IT person has unknowingly altered date and time stamps, overwritten useful deleted data, and skewed the original digital narrative of the intern's activity. In this instance, the intern's computer has been mishandled, making authentication an even greater hurdle down the road. While this evidence potentially held information that would have made the details of this event crystal clear, the IT person's involvement has made things murkier, and possibly not self-authenticating under the proposed additions to Rule 902.

So what should the IT person have done instead? Turn off the system as

quickly as possible and find a digital forensic expert for forensic preservation. While IT departments promote cybersecurity and technology policies, it is important to differentiate between IT services and digital forensics. The former is proactive or precautionary, and the latter is reactive (e.g. used in litigation).

Therefore, using forensic methodologies that leave the "crime scene" unaltered, so to speak, is key for ensuring compliance with Rule 902. Adhering to best practices in the collection of digital evidence is emphasized in the upcoming additions to Federal Rule 902. Relying on digital forensic professionals is necessary in ensuring the usability of digital evidence, as well as taking advantage of the lower burdens for authentication for it under Rule 902.

Digital evidence is an unbiased witness

Standardizing methods for the collection of electronically stored information is a big step toward recognizing the value of digital evidence as an unbiased witness. As society begins to move further away from "hard copies," this addition demonstrates the law's flexibility in accommodating our digital age. Unlike other types of information that may be collected for a trial, digital evidence is capable of presenting an unbiased record of activity. Admittedly, electronic evidence is not necessarily a complete repository of critical data, but think of the one device that most likely goes everywhere with you—your smart phone. I would argue that, for most of us, smartphones hold the most information about our day-to-day lives and much can be gleaned about our plans, intentions, and daily lives by reviewing their contents. The recent controversy over whether or not people should be forced to unlock their phones using a fingerprint illustrates exactly how protective people are of what is stored on their phones. With good reason, I often refer to phones as being like "snitches in our pockets." It doesn't matter how someone appears, how someone acts, or how convincing someone's story may be—digital evidence doesn't lie. Geolocation, text messages, emails, fitness applications, web browsing history, phone call logs, social media apps, and photos are only some of the ways that our phones offer glimpses into our lives. All of this information would be self-authenticating under the proposed 902(13), so long as it is certified by a qualified person.

Furthermore, the sheer volume of electronically stored information is constantly growing—creating an ocean of potentially useful data. As more and more is always being created, gathered, and stored on the vast number of diverse devices, litigants are presented with a huge amount and variety of potential evidence to use in court. Law enforcement is also faced with the problems posed by an influx of new technology, as data must be extracted from a variety of devices utilizing a number of different methods and tools. It would seem that as more emphasis is placed on digital evidence, it has become correspondingly difficult to gather, authenticate, and present in court. The revised Rule 902 responds to these issues for litigants by lowering the authentication hurdles.

Digital evidence can be open to interpretation

As an expert witness, I am frequently called upon to validate and explain digital forensic findings and their significance given the particulars of a case. Revealing hidden artifacts of long-forgotten digital activity is one thing—but constructing reliable narratives based on these facts and explaining their significance? Quite another. Questions of admissibility are only the beginning in establishing the value of electronic evidence. Making testimony understandable can be very difficult when computer lingo is a factor. And let's face it—computer people don't always have reputations for being effective communicators. And this is especially problematic, since oftentimes one piece of digital evidence can be the key that unlocks an entire case.

If it can be uncovered and related in an understandable way to a judge or jury, digital evidence is absolutely critical. Apart from the processes of uncovering data and ensuring its admissibility, the purpose of a digital forensic examination is to uncover a usable and understandable timeline, or narrative of digital activity. Ideally, forensic evidence is presented in such a way that it makes sense to everyone, not just the IT people in the room. Digital forensic experts are ultimately tasked with effectively explaining why a piece of evidence is significant, or possibly critical, in a case.

The expansion to include digital evidence in Federal Rule of Evidence 902 marks a definitive movement toward the standardization of data collection and authentication. No doubt, this will impact practitioners in federal court immediately, but also state court practitioners, as states commonly adopt rules that substantially track the federal rules. As such, this change underscores the need for digital forensic expert witnesses who can attest to both the authentication and significance of electronically stored information in both state and federal courts. While these changes go into effect on December 1 of this year, in reality, they are in place now. Following best practices for digital collection is now pertinent for any case going to trial after this date. ▲

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

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. ▲