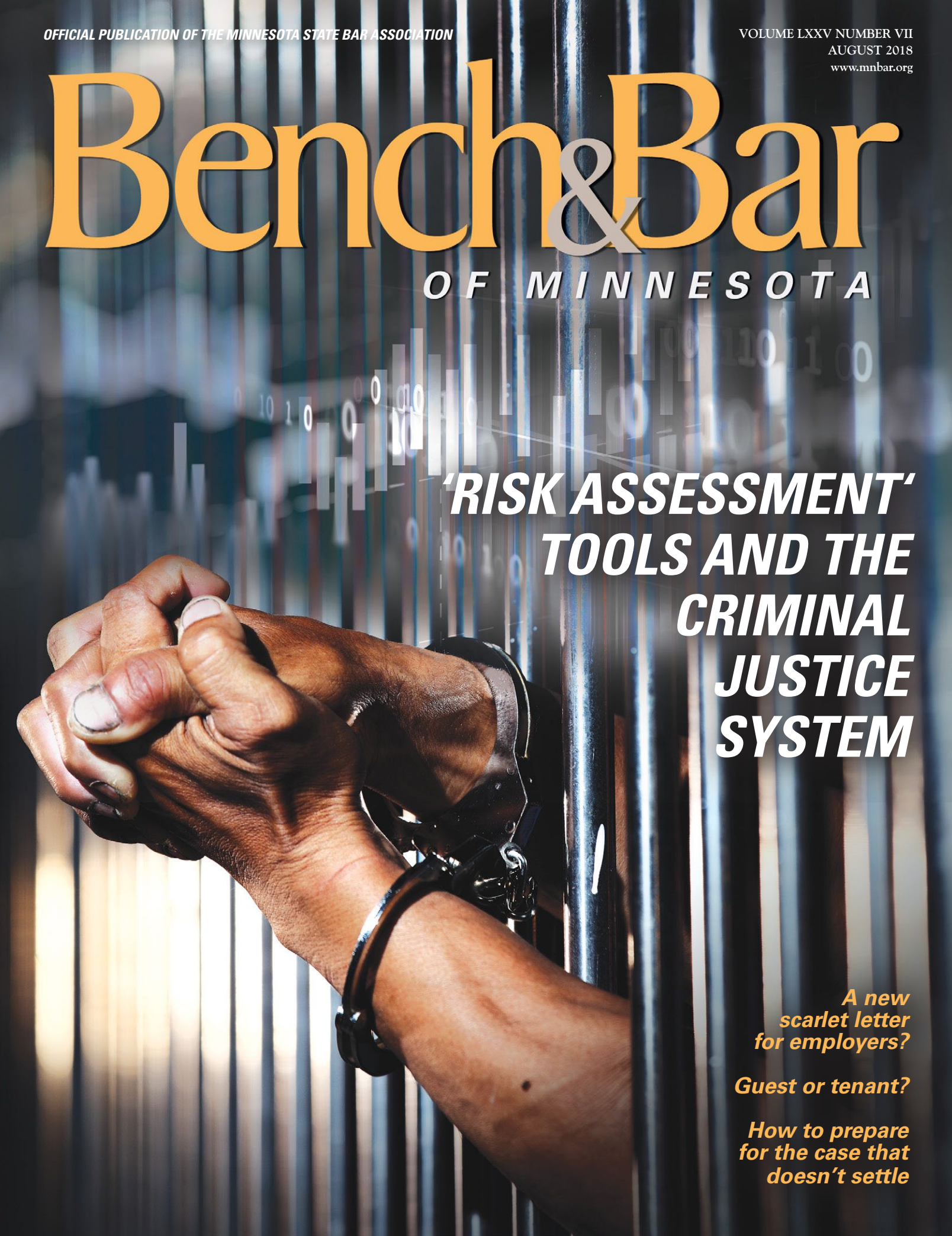
OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXV NUMBER VII
AUGUST 2018
www.mnbar.org

Bench&Bar OF MINNESOTA



'RISK ASSESSMENT' TOOLS AND THE CRIMINAL JUSTICE SYSTEM

A new scarlet letter for employers?

Guest or tenant?

How to prepare for the case that doesn't settle

E-discovery vs. forensics: Analyzing digital evidence

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

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

E-discovery versus forensics

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

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

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

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

No fishing expeditions

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

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

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