Practical and Ethical Considerations When Admitting Social Media and Other Electronic Evidence

Manvir Atwal
Federal Public Defender's Office
Minneapolis

Hon. Tanya M. Bransford
4th Judicial District
Minneapolis

Heidi J.K. Fessler
Barnes & Thornburg LLP
Minneapolis

Vicki J. Vial-Taylor
Hennepin Co Attorneys Office
Minneapolis

2017 Criminal Justice Institute – August 22 & 23, 2017

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.

E-Discovery has been a hot topic in the civil law arena for many years but it is just as important in the practice of criminal law. While it is commonplace to have large volumes of data to wade through in the typical white collar criminal matter, understanding and managing e-discovery is potentially important in all criminal cases. It is an inescapable reality that e-discovery plays a part in even routine criminal cases involving drugs, homicide, sexual assault and theft and at times this discovery can be voluminous in nature or complicated in the execution.

Criminal v. Civil E-Discovery

The rules governing civil and criminal discovery are fundamentally dissimilar due to the different public policies underlying criminal and civil litigation, constitutional requirements, and special ethical obligations of prosecutors and defense counsel. An essential difference between civil and criminal discovery is that of breadth: a criminal defendant is entitled to rather limited discovery, with no general right to obtain the statements of the Government's witnesses before they have testified. Fed. Rules Crim. Proc. 16(a)(2), 26.2. In a civil case, by contrast, a party is entitled as a general matter to discovery of any non-privileged information sought if it is relevant to the party's claims or defense and proportional to the needs of the case. Rule Civ. Proc. 26(b)(1).

In addition, criminal defendants are entitled to the effective assistance of counsel at trial and during plea negotiations. Defense counsel's effectiveness may depend on whether they have reviewed and understands the e-discovery in time to enter into informed plea negotiations. Criminal investigations and third-party subpoenas by both the prosecution and defense often bring vast quantities of ESI to criminal e-discovery. Complex ESI cases usually require litigation support resources not typically found in criminal defense practices.

E-Discovery can be a quagmire which traps the unwary lawyer resulting in sanctions, complaints and negative results. There may be endless systems, devices and repositories of data that may be arguably probative in a criminal case but there remain significant questions regarding the accessibility of such data as well as the impact that the collection of this data may have on personal and constitutional rights of the individuals. These questions are further compounded by

the lawyer's ethical obligations to the client. Criminal e-discovery matters because technology changes the rules of the legal ballgame. Increasing advances in legal technology are making it cheaper and easier for the government to conduct searches in criminal matters. To protect the public, while still respecting constitutional and civil liberties, the law, both civil and criminal, needs to keep pace with technology and attorneys need to raise their game.

Counsel Competency

One of the primary ethical obligations of counsel in the area of e-discovery is that of competency. The Minnesota Rules of Professional Conduct clearly apply to the handling of e-discovery by lawyers. Minnesota Rule of Professional Conduct 1.1, Competence, Comment [1], mandates that practitioners are expected to learn about e-discovery software and services or to associate with counsel of established competence in e-discovery when the need arises. Necessary study or association with competent counsel prior to the making of an expensive e-discovery request is a key to professionalism. (*See also* Minn. R. Prof'l Conduct 1.1, comment 8 (part of a lawyer's duty to provide "competent representation" includes "keep[ing] abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." [Amended June 11, 2015]).

Consider the implications, ethically and even criminally, of an attorney arriving at the crime scene of a homicide. Maybe the victim is still present at the scene. Perhaps the gun that delivered the fatal shot is still lying on the floor. Imagine the ethical implications if the attorney walks through the crime scene, picks up and examines the gun, maybe rifles through the victim's pockets and scrolls through the text messages on the victim's phone. Those same ethical implications are present, although not nearly as obvious, when an attorney handles digital data on a client's phone, computer, social media site or any device. Handling the data may well destroy the evidence through spoliation of metadata much like handling a gun at a crime scene may destroy fingerprints.

Discovery is an essential part of any case and even seasoned attorneys may lack the necessary knowledge and skills required to meet the rapidly changing challenges of e-discovery. The complexity involved in the identification, preservation and collection of data required by today's criminal matters require an enhanced knowledge of technology and data that may be beyond that possessed by the standard criminal attorney. To meet the competency requirement counsel may

need to associate with counsel providing a much deeper knowledge of data, information management systems, and/or network architecture. Understanding what devices and systems may contain relevant data, and how to access that data in a manner that preserves the data's forensic defensibility, requires a specialized skill set. Failing to obtain and handle data properly can often result in the inability to adequately authenticate the data resulting in its inability to be used as evidence at the trial of a criminal matter.

The increase in available data is fueled by the growing intrusion of technical data and devices into everyday life. This technical proliferation results in an ever-increasing sea of data which may ultimately prove probative in a criminal matter. The standard smartphone, and any number of applications thereon, is constantly tracking your location to within a few feet. The blackbox within your car is recording not only the performance and condition of the car but also the application of the brakes, vehicle speed and even if the lights or radio are in use. Beyond the issues raised by data on personal devices, there are myriad external and third party devices and systems capable of tracking and recording individual activities. For example, today's thermal imaging devices can be used to identify and document marijuana growing operations without the need for law enforcement to even step foot on the premises.

Courts are already facing the challenges posed by the new devices and the data created by these devices. A recent criminal case out of Arkansas, State v. Bates, illustrates this fact quite well. In State v. Bates, a few friends, one of whom was Bates, spent an evening drinking and watching football at Bates' residence. When the morning light hit the hot tub, the body of one friend was discovered floating lifeless. Bates, the owner of the residence, called 911 and the police arrived on the scene. During the investigation, the police noticed what appeared to be signs of a struggle in the area and suspected homicide. Police proceeded to obtain a search warrant for the residence.

When police entered the Bates' home, pursuant to the search warrant, they noticed an array of "smart" devices including a Nest thermostat, a wireless home alarm system, wireless weather monitoring station and an Amazon Echo. The police seized the Amazon Echo as they stated that they had reason to believe that it may contain words or audio related to the suspected homicide.

By way of explanation, the Amazon Echo is one of a new breed of "smart" electronic home devices that essentially listens for audible commands at all times. The Amazon Echo is a wireless speaker and voice command device with a seven-piece collection of microphones that operates the Alexa Voice Service. A user sets the device to recognize a wake word, choosing between the two pre-set options of either "Alexa" or "Echo". Once the device hears the designated wake word it will begin recording the user's audio requests, execute commands and offer helpful advice. Once the device hears the wake word, and actually for a fraction of a second prior to the wake word as the device is always listening, the Echo beings streaming the recorded audio to the designated cloud repository. Once in the Amazon cloud, the recording and transcription of the audio is logged and stored in the Amazon Alexa app and must be manually deleted. The system retains the time and content of all audio within the system.

The police, seeking the data communicated from the Alexa device to the Amazon cloud, requested that Amazon provide the data and served Amazon with a search warrant. Amazon refused to comply with the search warrant and sought to quash the warrant. The controversy became moot when Bates agreed to allow Amazon to release the data from his Echo device to the prosecutors.

In another technology twist, the investigators in State v. Bates also recovered digital data from a specialized water meter with hourly water usage computations that would be used by the prosecution to show Bates's inordinate consumption of water during a one-hour period which they will suggest resulted from his washing blood from the crime scene.

This type of evidence wouldn't have even existed just a few years ago and the collection and preservation of such evidence requires specialized technical knowledge. Failing to recognize the existence of such evidence, as well as the special handling required by such evidence, can result in mistakes, ethical failings and complaints.

Restrictions on Criminal Discovery

Criminal discovery is more restricted than civil discovery. The Constitution provides criminal defendants with several discovery-related procedural protections including the right against self-incrimination and the right to confront witnesses. Because of these constitutional guarantees,

criminal discovery tends to be rather unbalanced. For example, under the U.S. Supreme Court's decisions in *Brady v. Maryland* and *Giglio v. United States*, the prosecution must turn over to the defendant all exculpatory and impeachment evidence in the government's possession. A criminal defendant has no equivalent duty because of the right against self-incrimination. Additionally, in jurisdictions that require limited forms of pretrial disclosures or court-ordered depositions, requesting evidence in possession of a defendant may be useless; any evidence in the defendant's possession that tends to support a finding of guilt is protected by the constitutional right against self-incrimination. Therefore, while the prosecution is frequently ignorant of the defense's evidence, the defense should be well-versed in the prosecution's evidence. In essence, although police and prosecutors can search and seize your data in a criminal matter, rather than going through the niceties of a document request, the Fourth Amendment will often provide extra protection for the person being investigated, requiring police and prosecutors to obtain search warrants.

Social Media Data in Criminal Matters

Access to Social Media

The pervasive reach of social media has resulted in social media evidence becoming ubiquitous in criminal matters. A survey of court decisions published in just January 2017, where social media evidence played a meaningful role in the litigation, is in excess of 1200. (https://blog.x1discovery.com/2017/02/08/criminal-conviction-overturned-due-to-failure-to-authenticate-social-media-evidence/). In addition, Social media has become an important tool for law enforcement officials who use it for everything from enabling witness identifications of suspects, investigating gang affiliations to going undercover to gather evidence against suspected criminals. Defense attorneys are also using this data and social media sites to mine for information on their clients, witnesses, and other key players. In fact, a number of jurisdictions have begun holding attorneys to a higher standard when it comes to making use of online resources, including demonstrating due diligence and even locating and using exculpatory evidence in criminal cases. *Cannedy v Adams*, 706 F.3d 1148 (9th Cir. 2013) (holding that a lawyer's failure to locate a sexual abuse victim's recantation on her social media profile could constitute ineffective assistance of counsel).

How counsel actually obtains social media information can raise some interesting ethical voncerns. While there generally is no ethical prohibition against an attorney (or someone working for that attorney) viewing the publicly available portion of an individual's social networking profile or social media site, they may not try to "friend" someone in order to gain access to the privacy-restricted portions of that profile? Ethics opinions form the Philadelphia Bar Association (March 2009), the New York City Bar (September 2010), the New York State Bar (September 2010), the Oregon Bar (February 2013) the New Hampshire Bar (June 2013), and others have made it clear that the rules of professional conduct against engaging in deceptive conduct or misrepresentations to third parties extend to cyberspace as well. As the New York City Bar ethics opinion emphasizes, with deception being even easier in the virtual world than in person, this is an issue of heightened concern.

Preservation of Social Media

What is a criminal defense attorney to do, if, during a meeting with a client, the client informs counsel that there are numerous photographs on his Facebook profile of him taking drugs, brandishing weapons, or engaging in other illegal activities? Should the lawyer advise the client to delete the Facebook page? Although some have taken this route to their detriment, lawyers who choose this course of action will run afoul of both their ethical obligations and the law. Under Rule 3.4 of the Model Rules of Professional Conduct (Fairness to Opposing Party and Counsel), lawyers may not "unlawfully . . . destroy or conceal a document or other material having potential evidentiary value," nor may they counsel any other person to do so. (emphasis added.) The commentary to the rule clarifies that the prohibition "applies to evidentiary material generally, including computerized information," and to information that has potential evidentiary value to "a pending proceeding or one whose commencement can be foreseen." (emphasis added.) Moreover, destroying evidence relevant to pending litigation—or causing someone else to do so—is a criminal offense in addition to being an ethical violation. For these reasons, lawyers should exercise great caution when advising clients about the possibility of deleting potentially relevant social networking materials.

One notable case where the attorney for a party provided the wrong advice to a client regarding the deletion of data from a social media account is the case *Allied Concrete Co. v. Lester*, 736 S.E.2d 699 (Va. 2013). Lester was a recent widower as the result of a tragic car/truck accident

which killed his then 25 year old wife. The lawsuit against the driver of the truck and his employer resulted in a massive $10.6 million verdict to Lester. Unfortunately for Lester and his counsel, roughly a year later, a judge issued a final order cutting that verdict in half and issuing additional sanctions against Lester and his counsel totaling $722,000.00. Of that total, Lester was obligated to pay $180,000.00 and his counsel to pay $542,000.00. The court, in providing its rationale for the sanctions stated; "Whereas, the court, having reviewed the evidence and arguments of counsel and carefully considered the extensive pattern of deceptive and obstructionist conduct of Murray and Lester resulting in the sanction award". The obstructionist conduct giving rise to the sanctions began in March of 2009 when Murray, counsel for Lester, received a request for the contents of Lester's Facebook account. The request was accompanied by a photo, clearly taken from Lester's Facebook page, showing Lester partying with buddies and wearing a t-shirt emblazoned with the message "I [heart] hot moms". Murray, through his paralegal, advised his client to "clean up" the Facebook page and eventually told him to deactivate the page the day that Lester signed the discovery responses. It was found that Lester deleted a total of 16 photos prior to producing material to defense counsel. More shenanigans ensued and culminated in Murray leaving the practice of law.

The depth of the information found on social media sites is staggering. Not surprisingly, social media posts can contain admissions or incriminating photos in addition to other evidence. Just on Facebook alone, the available information may include the user's profile information, wall posts, photos that the user uploaded, photos in which the user was tagged by other Facebook users, GPS or location data and timestamps on the acquisition of that location data, a comprehensive list of the user's friends and their Facebook IDs as well as a long table of login and IP data. Take the case of John McAfee who, while on the run from possible murder charges, posted a "selfie" on his blog. He was forced out of hiding when it was discovered by law enforcement that the "selfie" contained embedded GPS data pinpointing his exact location in Guatemala.

The ethical challenge facing counsel is that they must understand the process of e-discovery to be able to manage it. They must possess the requisite competency to employ the proper collection and preservation techniques needed to obtain the social media data in a manner that permits the authentication of the data and preserves the data and metadata needed to lay the foundation for its introduction into evidence. If an attorney does not personally possess the

specialized knowledge required for e-discovery they are ethically required to seek out the assistance of attorneys who do possess this specific skill set. An attorney cannot merely hand off the decisions and should stay engaged to ensure that they have performed all of their supervisory responsibilities. Taking a photograph may not be enough, a simple screenshot may not work and it generally requires specialized tools and technology to obtain the social media data with the requisite metadata intact and unaltered. It is important for counsel to work with skilled resources who understand the need to memorialize each step of the collection and production process in addition to considering how counsel will ultimately seek to authenticate the tweet, Facebook post, Instagram photo or blog post.