

**IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF
MARYLAND**

STATE OF MARYLAND

vs.

ALAKOM-ZED CRAYNE POBRE

Defendant.

Case No.: 8:19-cr-00348-PX

**AFFIDAVIT OF MARK LANTERMAN IN SUPPORT OF DEFENDANT’S
MOTION TO COMPEL**

STATE OF MINNESOTA)
) *ss.*
COUNTY OF HENNEPIN)

Mark Lanterman, being first duly sworn, states as follows:

1. My name is Mark Lanterman. I am the Chief Technology Officer of Computer Forensic Services (“CFS”) located in Minneapolis, Minnesota. CFS and I have been retained by counsel for Defendant Pobre to assist with technical matters related to the Freenet network, and specifically the investigative technique(s) utilized by law enforcement in its pre-warrant investigation in this case.

2. Consistent with my opinions outlined in greater detail in this affidavit, the Government’s productions related to its modified version of the Freenet software are insufficient to evaluate the reliability of the technique(s), in general and as applied in its investigation here.

Expert Background

3. Our firm specializes in the analysis of digital evidence in civil and criminal litigation. I have over 25 years of experience in computer forensics and cybersecurity. Prior to joining CFS, I was a sworn investigator for the United States Secret Service Electronic Crimes Task Force and acted as its senior computer forensic analyst.

4. I am certified by the United States Department of Homeland Security as a “Seized Computer Evidence Recovery Specialist,” as well as certified in computer forensics by the National White-Collar Crime Center. Both federal and state court judges have appointed me as a neutral computer forensic analyst or special master.

5. I graduated from Upsala College in New Jersey with both a Bachelor of Science and a Master’s degree in computer science. I completed my post graduate work in cyber security at Harvard University.

6. I am currently adjunct faculty of computer science for the University of Minnesota Technological Leadership Institute’s Master of Science and Security Technologies program (MSST). I am also faculty at the Mitchell Hamline School of Law (in Minnesota) and a professor of cybersecurity at the University of St. Thomas School of Law (in Minnesota). I am also faculty for the National Judicial College in Reno, Nevada and the Federal Judicial Center in Washington, D.C.

7. I have previously provided training or delivered keynote addresses for the United States Supreme Court; the Eleventh Circuit Federal Judicial

Conference; the Eighth Circuit Federal Judicial Conference; the Southern District of Georgia; the Western District of Tennessee; and several state judicial conferences. I delivered the keynote address at the Chief Justices' Conference in Newport, Rhode Island and at Georgetown Law School's e-discovery conference.

8. I was appointed by the Minnesota Supreme Court to serve as a member of Minnesota's Lawyers Professional Responsibility Board ("LPRB"). I currently serve as chairman of the LPRB's Opinion Committee.

9. CFS and I were retained to evaluate the source code of the Intoxilyzer 5000EN machine, which was used to measure blood-alcohol content after DUI arrests, on behalf of defense attorneys and their clients in Minnesota who had raised concerns regarding the accuracy of the Intoxilyzer's source code. After conducting the source code analysis ordered by Federal District Court Judge Donovan Frank, CFS and I ultimately determined that the source code, and consequently the device, operated as designed.

10. I am a co-author of the Minnesota State Bar's e-Discovery Deskbook, and I also write monthly articles for *Minnesota Bench & Bar* magazine.

11. CFS is the exclusive, contracted computer forensic service provider for the Hennepin County Sheriff's Office (the county that encompasses Minneapolis); the Ramsey County Attorney's Office (the county that encompasses St. Paul); the Washington County Attorney's Office in Minnesota; as well as the Metropolitan Airports Commission, also known as the Minneapolis/Saint Paul International

Airport. CFS is also partnered with the U.S. Secret Service to assist with its electronic investigations.

12. I have attached a list of cases in which I have testified in the last four years, as well as a list of articles I have written for a number of publications throughout the past 10 years. I am compensated at a rate of \$625 per hour. My compensation is not dependent upon the outcome of this case.

Documents Reviewed

13. I am familiar with the general procedural history of this action, and the facts as alleged. In preparing this affidavit, counsel for Defendant has provided me with the following documents, which I have reviewed and that form the factual basis for my opinions outlined in this affidavit:

- a. Defendant's Memorandum in Support of Motion to Compel, dated February 3, 2020;
- b. Government's Response to Defendant's Motion to Compel Discovery, dated February 26, 2020.
- c. "A Forensically Sound Method of Identifying Downloaders and Uploaders in Freenet," Dr. Brian D. Levine, et al.
- d. Defendant's Motion to Suppress Physical Evidence, dated August 17, 2020;
- e. Defendant's Motion for Franks Hearing, dated August 17, 2020, and associated exhibits;
- f. Defendant's Consolidated Memorandum in Support of Motion to Suppress and Reply to Motion to Compel, dated August 17, 2020, and associated exhibits (including the search warrant(s), "Freenet Target Summary," and "Statistical Detection of Downloaders on Freenet");

14. I reserve the right to supplement or amend this affidavit should additional information be made available to me, or the circumstances, related to the issues about which I have been retained to provide assistance, change.

Overview of Government’s Freenet Investigation Technique

15. Based upon the materials that have been made available to me, the Government’s process for investigating the movement of contraband on Freenet is, essentially, a three-step process. For ease of reference, the process briefly described below will be referred to as the “Government investigative technique.”

- a. First, the Government records requests for data (files) that are transmitted over Freenet and happen to traverse its Freenet nodes, which participate in Freenet to receive requests.¹ Detailed information about incoming requests are “logged” or recorded.² This add-on mechanism preserves information that is otherwise not captured using the standard consumer Freenet software. (See Gov’t Resp. at 4-5). The added functionality is “...a simple modification of the Freenet software” that essentially acts as a scratchpad, writing down data about data transmissions that happen to be received by Government

¹ See Def.’s Consolidation Memo. In Supp. Of Motion to Suppress fn 1, “A node is a computer that is running the Freenet program.” (citing *United States v. Dickerman*, No. 4:16-CR- 00258-HEA-NAB-1, 2017 U.S. Dist. LEXIS 226787, at *5 n.2 (E.D. Mo. Sep. 26, 2017)).

² See also *United States v. Dickerman*, No. 4:16-CR- 00258-HEA-NAB-1 (E.D. Mo. Sep. 26, 2017) at 5, “These ‘observations’ include: the IP address of the peer; the Freenet “location” of the peer; the block, identified by the SHA256 hash value; Hops to Live (HTL); time stamp; an identifier that uniquely identifies the law enforcement node connected to the peer; the number of peers the observed peer reports itself to have; and ‘other information that is visible to any of the node’s peers’.”

Freenet nodes. (See Levine Depo. at 55 lns. 6-7, *U.S. v. Hall*, Crim. Case No. JFM-16-469 (Aug. 30, 2017)).

- b. Second, law enforcement has “collected the manifests to suspected child pornography files that are publicly shared and created a database of the associated keys to the blocks of a file.” (See App. for Search Warrant at 10). As an analogy, law enforcement has assembled the collection of instructions (manifest keys, and hash values of individual blocks of files representing contraband) that Freenet uses to route encrypted pieces of a file back to a requestor for reassembly.³ Recorded information collected using the Government’s modified Freenet software is compared to this database so that requests for contraband may be identified and subsequently investigated. (*Id.*).
- c. Third, once recorded data is identified as potentially relating to contraband, the Government uses that information to conduct a statistical analysis to determine whether a recorded request passed to a Government Freenet from an original requestor or a “relayer.” (See *generally* “A Forensically Sound Method of Identifying Downloaders and Uploaders in Freenet” § 3(B-E), Fig. 1).

The Government’s Investigative Technique As Applied

16. I understand that the Government presented its results of the above-simplified process as a synthesized, one-page document, titled simply “Freenet

³ A hash value is like a digital fingerprint—an alphanumeric string that can be used to identify unique files. See *also supra*. fn 2.

Target Summary.” (See Def.’s Consolidated Memo. in Supp. of Mot. to Suppress Ex. 3). I further understand that this document was used to support the search warrant in this case.

17. The Freenet Target Summary document discloses that at least four Government Freenet nodes recorded information about the data requests that supported the search warrant in this case.⁴ The document does not represent the unmodified output generated and recorded by the modified Freenet software, but rather a synthesized, consolidated amalgam of information collected by the four Government nodes, ostensibly using the function(s) documented by Dr. Levine. (See generally “A Forensically Sound Method of Identifying Downloaders and Uploaders in Freenet” § III(C)).

18. In other words, the original, both the unmodified data that was relied upon to generate the Freenet Target Summary document, to my knowledge, has not been produced. For this reason, the Freenet Target Summary document does not provide any demonstration of the reliability and completeness of the underlying data.

Collected data has apparently not been produced about the subject requests for contraband.

19. First, and most glaringly from the materials that have been made available to me, it is apparent that additional information may have been collected

⁴ The Government’s Freenet nodes are identified as “LE # 1809,” “LE # 1921,” “LE # 2145,” and “LE # 2161.” (See “Freenet Target Summary,” Def.’s Consolidated Memo. in Supp. Of Mot. To Suppress Ex. 3).

pertaining to the transmissions that were the subject of the search warrant. (*See supra* fn. 2, *see also* “A Forensically Sound Method of Identifying Downloaders and Uploaders in Freenet” § III(E), “Requests contain the key, an HTL, the sender’s IP address and Freenet location, and the request type...”). Indeed, it is expected that additional data about the transactions was recorded at the time the requests were allegedly made. This additional information is not summarized or contained within the Freenet Target Summary document.

20. Other data about the requests is critical and may provide useful context for the data presented in the Freenet Target Summary document. By way of example and not limitation, additional recorded data may be available such as the transmissions’ hops-to-live (HTL) count, and whether the subject computer was using Freenet in “opennet” or “darknet” mode.⁵

21. The HTL count would show how many other peers a request “hopped” to or traversed through before arriving at a Government node, which would tend to differentiate whether the transmission was a direct request, or whether it was a relayed request. The HTL count can be thought of as a request’s fuel tank, demonstrating how far the request has travelled. Dr. Levine highlights the importance of the HTL count, writing, “[b]ecause of Freenet’s policy for decrementing HTLs and its defined maximum HTL of 18, we can assume that

⁵ *See* “A Forensically Sound Method of Identifying Downloaders and Uploaders in Freenet” § II, “In opennet, nodes connect to other open nodes... In darknet, Freenet nodes connect only to peers for which the user has explicitly given permission...To prevent block requests from propagating indefinitely, Freenet uses a *hops-to-live* (HTL) counter....the HTL is decremented by each relay node until it is zero, in which case a not-found error is returned)].

requests with an HTL of 16 or below did not originate with neighbors.” (*Id.* § V(B)). Simply, if the “fuel tank” of a Freenet request is less than full, it can be inferred that it was not a direct request, but rather one that has made previous “stops.”

22. The mode that the user used Freenet in is also of critical importance because it would indicate whether the Government would have had to take affirmative steps to become a trusted peer of the subject node.

23. The above-listed examples are not all inclusive of the data that is not represented by the Freenet Target Summary document but are simply provided to describe categories of data that are missing wholesale. In short, because the Government has not provided all data related to the requests for contraband it observed here, it is not possible to evaluate the recorded information (as it is synthesized in the Freenet Target Summary document) in context or for its accuracy and reliability.

It cannot be ascertained whether the Government’s modified Freenet software reliably recorded and isolated investigative data about this case.

24. Second, it is not known whether the Government’s modified Freenet software does anything to change or modify the data after it passes to a Government Freenet node with the modified software installed, or if it records the data in *exactly* the same form as it traversed Freenet. While the Government’s modified Freenet software has been described as simply a mechanism “to write [information about incoming requests] down,” it is not ascertainable whether the software annotates or categorizes the data in order to simplify the process of determining which values/variables to plug into the mathematical functions. As an

example, it is not ascertainable from the data that has been made available to me, to determine whether the Government modified Freenet software identifies an IP address, or a manifest key, or any other piece of information and denotes it as such in its output.

25. Whether the Government modified Freenet software changes data is significant because it introduces the possibility that data may be either inaccurately recorded by the software, or later misattributed. Indeed, it is further unascertainable whether the software comingled the investigative data here with data about other connections that passed to the Government's nodes. For example, if data is comingled with data about other requests, a request for a block of a file representing contraband may be mistakenly attributed to an IP address that has nothing to do with the request.⁶

26. If the software categorizes or comingles data, there is risk of cross pollination and inaccurately attributed results. (*See* Gov't Resp. at 12, "...the investigative software contains sensitive details regarding hundreds—if not thousands—of active investigations around the United States and the rest of the world, including information about IP addresses under investigation and suspected physical addresses...).

27. More generally, it is not determinable without an analysis of the source code and its output in this case, to determine if the *only* feature of the

⁶ I note that the Freenet Target Summary document shows that rows are "filtered," suggesting that the population of collected data requests is larger than those represented by the Freenet Target Summary document.

Government modified Freenet software is “writing down” information about incoming requests that happen to pass through to the Government’s own Freenet nodes, or if the software has other coded solutions to assist the Government automate its investigations. For example, based upon my review of the documents, the Government modified Freenet software may do more than simply “write down” information about connections. It may also distinguish between requests for contraband, and non-contraband.⁷ These details bear directly on the reliability of those other feature(s), if any.

28. Without access to all source code and its complete output that was used to support the search warrant in this case, it is not possible to verify whether the software operated as intended. In my opinion, the above described factors—namely, the apparent absence of produced data related to the requests, and the precise extents of the functionality of the Government modified Freenet software—justify validation testing and analysis of the software and its output. Consequently, at this juncture, I respectfully request:

- a. the modified Freenet software utilized in this case;
- b. to the extent it was used in the pre-warrant investigation in this case (or otherwise not a function of the modified Freenet software), any secondary software or tool used to identify activity potentially related

⁷ While Levine notes that, in his testing, “[his] nodes were modified to log only the requests whose keys matched those [of child exploitative material];” it is not clear whether that was the case for the Government modified Freenet software was deployed here. There are suggestions that the software may have been more inclusive of requests about which it recorded information, because the Government’s filings refer to “requests” generally and not to requests for contraband specifically. (See Gov’t Resp. at 4-5, “This law enforcement version is nearly identical to Freenet, except that it allows a computer operated by a law enforcement officer to automatically log information about requests for pieces of files received directly from its peers.”, *see also see also* App. for Search Warrant at 10, “Law enforcement Freenet nodes record requests that are sent to them...”)

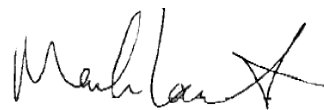
to contraband, and as collected by the Government's modified Freenet software;

- c. copies of the original, unmodified output from that software as deployed on the multiple law enforcement Freenet "nodes" used to support the search warrant in this case;
- d. to the extent that it was used, any software, template or tool containing the formulas used to interpret the harvested Freenet data (or, in other words, used to create the Freenet Target Summary document);
- e. any and all documentation (user manuals, help guides, or training materials) about the software and its configuration on the law enforcement Freenet nodes.

29. If provided with the above-listed information, CFS and I would conduct an analysis of the materials to validate the software and its output as the technical circumstances dictate.

30. I understand that the Government has previously objected to Defendant's requests for the source code. CFS and I agree to not share any materials related to this case absent any directions from the Court.

I declare under penalty of perjury under the law of the United States that the foregoing is true and correct.



Mark Lanterman



Mark Lanterman Chief Technology Officer

Office
800 Hennepin Avenue
5th Floor
Minneapolis, MN 55403

Phone
(952) 924-9920

Fax
(952)924-9921

Email
mlanterman@compforensics.com

Web
www.compforensics.com

Professional Biography

Mark has over 25 years of experience in digital forensics, e-discovery, and has provided education and training to a variety of audiences. Prior to founding Computer Forensic Services in 1998, Mark was a sworn law enforcement investigator with the United States Secret Service Electronic Crimes Task Force. Both federal and state court judges have appointed Mark as a neutral computer forensic analyst.

Mark is a member of the Minnesota Lawyers Professional Responsibility Board and serves as Chairperson of its Opinion Committee.

Mark frequently provides training within the legal community, including presentations for the United States Supreme Court, Georgetown Law School, the 11th Circuit Federal Judicial Conference, the 8th Circuit Federal Judicial Conference, the American Bar Association, the Federal Bar Association, and the Department of Homeland Security, among others.

As a member of its faculty, Mark has presented to the entire Federal Judiciary through the Federal Judicial Center. Mark is faculty at the National Judicial College, Mitchell Hamline School of Law, and is an adjunct instructor in the University of Minnesota's MSci Security Technologies program. Mark is also a professor at the Saint Thomas School of Law.

Mark provides frequent commentary about cyber security issues for national print and broadcast media, including ABC, Bloomberg, BusinessWeek, CBS, Fox News, NBC, *The New York Times*, NPR, and the *Wall Street Journal*.

Education and Certifications

Upsala College - B.S. Computer Science; M.S. Computer Science

Harvard University - Cybersecurity

Department of Homeland Security - Federal Law Enforcement Training Center
Seized Computer Evidence Recovery Specialist

National White-Collar Crime Center - Advanced Computer Forensics

Publications

Co-author of the *E-Discovery and Forensic Desk Book*

Regular columnist for *Bench & Bar* magazine



Previous Testimony List – Mark Lanterman

- In re: Estate of Anthony Mesiti, 318-2017-ET-00340, N.H. 6th Cir. Probate Division. (2020)
- Ernie’s Empire, LLC, et al. v. Burrito & Burger, Inc., et al., 82-CV-20-28, (Wash. Co., Minn.)
- Sol Brandys v. Wildamere Capital Management LLC, Case No.: 27-CV-18-10822, (Henn. Co., Minn.)
- State of Minnesota v. Yildirim, Case No. 27-CR-19-7125, (Henn. Co., Minn.)
- Jabil v. Essentium, et al., Case No. 8:19-cv-1567-T-23SPF, (U.S. M.D. Fla.)
- Lifetouch National School Studios Inc. v. Walsworth Publishing Company, et al., (U.S. Dist. Conn.)
- Motion Tech Automation, LLC v. Frank Pinex, Case No.: 82-CV-18-5202, (Wash. Co., Minn.)
- Lundin v. Castillo, et al., Case No.: 2019-CV-000452, (Walworth Co., Wis.)
- Yun v. Szarejko-Gnoinska, et al., Case No.: 27-PA-FA-13-967, (Henn. Co., Minn.)
- Jonas Hans v. Belen Fleming, Case No.: 27-PA-FA-13-967, (Henn. Co., Minn.)
- Daniel Hall, et al. v. Harry Sargeant III, Case No.: 18-cv-80748, (U.S. Dist. Ct. S.D. Fl.)
- Miller v. Holbert, et al., Case No.: 48-CV-15-2178, (Mille Lacs Co., Minn.)
- Strohn, et al. v. Northern States Power Company, et al., Case No.: 18-cv-1826-DSD-KMM, (U.S. Dist. Ct. Minn.)
- Stamper, et al. v. Highlands Regional Medical Center, Case Nos.: 11-CI-1134 & 12-CI-00468, (Commonwealth of Kentucky, Floyd Cir. Co., Div. I).
- Patterson Dental Supply, Inc. v. Daniele Pace, Case No.: 19-cv-01940-JNE-LIB, (U.S. Dist. Ct. Minn.)
- Ryan Rock v. Jonathan Sargent and The Sargent Group, Inc. d/b/a Todd & Sargent, Inc., Case No. LACV050708, Dist. Ct. Story Co., Iowa.
- Oscar Alpizar v. Eazy Trans, LLC, et al., Case No.: 2018CI00878, (Dist Ct. Bexar Co., Texas)
- MatrixCare v. Netsmart, Case No.: 19-cv-1684, (D. Minn.)

- State of Minnesota v. Nathan Roth, Case No.: 80-CR-18-1007, (Wadena Co., Minn.)
- Parisi v. Wright, Case No.: 27-CV-18-5381, (Henn. Co., Minn.).
- Lloyd C. Peeoples, III v. Carolina Container, LLC, U.S. N. Dist. Geor., Case No.: 4:19-cv-00021
- Sandra Wolford, et al. v. Bayer Corp., et al., Action No. 16-CI-907, 17-CI-2299, Commonwealth of Kentucky, Pike Cir. Ct. Div. I. (2019)
- BuildingReports.com, Inc. v. Honeywell International, Inc., Case No.: 1:17-cv-03140-SCJ, (U.S. Dist. Ct. N.D. Ga.)
- Evan D. Robert and Dr. Kerry B. Ace v. Lake Street Cafeteria, LLC, et al., Case No: 27-CV-17-18040, (Henn. Co., Minn.)
- State of Minnesota v. Andrew Seeley, Case No.: 14-CR-17-4658, (Clay Co., Minn)
- McNutt & Company v. Focus Engineering, et al., Case No.: CV-2018-900432.00, Cir. Ct. Lee County, Alabama.
- In re: City of Eden Prairie and Law Enforcement Labor Services Inc., BMS Case #19-PA-0530 (2019).
- State of Minnesota v. Stephen Allwine, Case No.: 82-CR-17-242, (Wash. Co., Minn.)
- PMT v. Wade Fredrickson, Case No.: 27-CV-18-4364, (Henn. Co., Minn.)
- Stratasys, Inc. v. Christopher Krampitz, Case No.: 0:17-cv-05524-DSD-HB, (D. Minn.)
- State of North Dakota v. Connor Brennan, (Court File No.: 17300214), (Grand Forks Co., ND)
- U.S. v. Farber, Case No.: 1:2017-cr-00188-320735, (E.D. Cal.)
- In re: the Marriage of: Amanda Jo Briggs and Kent Stewart Mitchell Briggs, Case No.: 27-FA-17-3414, (Henn. Co., Minn.)
- Edgewell Personal Care Company v. Michael O'Malley, (Superior Court (Judicial District of Ansonia at Milford) No. AAN-CV-176025160-S)
- East Coast Test Prep, L.L.C. d/b/a Achieve Test Prep and Mark Olynyk, v. Allnurses.com, Inc., and David R. Smits, as Administrator of the Estate of Brian Short, ABC Companies 1-10 and John Does 1-10, Case No.: 0:15-cv-03705-JRT-SER (D. Minn.)
- DTN, LLC, v. Matthew Walsh, Case No. 0:17-cv-5206(SRN)(HB) (D. Minn.)
- In Re the Matter of: Wainaina Kamau and Ruth Marionya Kamau, Court File No: 27-DA-FA-18-5521 (Dist. Ct. Hennepin County, Minn.).
- Nagios Enterprises, LLC, vs. Mary Starr, et al. Court File No: 62-CV-16-3280, (Dist. Ct. Ramsey County, Minn.)

- Larry Novack v. David Rios and United Parcel Service, Inc. (TX Dist. CT., 57th Dist. (Bexar County, Texas) No. 2016-CI-12388)
- Mylan Pharmaceuticals Inc., Petitioner v. Sanofi-Aventis Deutschland GMBH Patent Owner (United States Patent and Trademark Office) U.S. Patent Nos. 7,476,652 and 7,713,930-IPR2017-01526/IPR2017-01528)
- Elisabeth Ostendorf v. Michigan State University and the Board of Trustees of Michigan State University, (State of Michigan (In the court of claims) No. 15-47-MZ)
- Elyse Puklich v. Blayne Puklich, (Burleigh Co., ND) No. 08-2014-CV-00029)
- Miles Construction, Inc. v. Andrea Weisberg and Daniel Rutman, (MN Dist. CT., 4th Dist. (Hennepin Co.) No. 29-cv-16-14404)
- Jeffrey Ketchum and Anniken Ketchum vs. Home-Owners Insurance; D & L Janitorial Supply, Inc. (MI 47th Circuit Court (Delta Co.) No. 15-22960-CB)
- Parsons Electric L.L.C vs. Integrated Building Solutions L.L.C., Paul Kelly, Kristopher Kelly, Troy Stanislawski, and Jack Tucker (MN Dist. CT., 10th Dist. (Anoka Co.) No. 02-CV-16-2644)
- State of Minnesota vs. Erin Marie Hennessey, (MN Dist. CT., 10th Dist. (Washington Co.) No. 82-CR-16-2208)
- The Hays Corporation vs. Barry Peters, et al. (In The Circuit for Montgomery Co., Maryland)
- International Chemtex Corporation vs. Jennifer Lassiter, John Hofstad, and Sustainable Water Treatment, LLC (United States Dist. Court (Dist. of MN)
- David Rubenzer and La La La, LLC vs. City of Burnsville (MN Dist. CT., 1st Dist. (Dakota Co.) No. 19HA-CV-15-3743)
- State of Minnesota vs. John Frederick Thorene, IV (MN Dist. Ct., 6th Dist. St. Louis Co.) No. 69DU-CR-15-3038)
- Nu-Look Exteriors, Inc. vs. Brett A. Looney, Mark A. Peare, Julie A. Young, f/k/a Julie A. Strot, Stephen B. Martin, and 4 Corner Architectural Sheet Medal, Inc. (MN Dist. CT., 1st Dist. (Dakota Co.) No. 19HA-CV-15-432)
- Brook Mallak v. Aitkin County, et al., (United States District Court of Minnesota, No. 13-CV-02119 DWF/LIB)
- Jonathan Scarborough v. Federated Mutual Insurance Company, (United States District Court (Dist. of MN) No: 0:15-cv-01633 -DWF/FLN)
- Future Motion, Inc. vs. Changzhou First International Trade Co., LTD, (United States District Court (Dist. of NV) No. 2:16-cv-00013-MMD-CWH)
- In re the Marriage of: Catherine Ann Ivey and John Raymond Ivey, (State of Minnesota (Hennepin Co.) No. 27-FA-15-7650)

- Bay Side Recycling Co., et al. v. SKB Environmental, Inc., Case No.: 14-CV-4550 (SRN/LIB), (U.S. Dist. Ct. Minn.).
- United States of America v. Khaalid Adam Abdulkadir, (United States District Court (Dist. of MN) No: 15-mj984 KES)
- Kimberly Kay Seidel and Trevor Carlton Seidel, (MN Dist. Ct., 10th Dist. (Anoka Co.) No. 02-FA-15-2022)
- Dexon Computer, Inc. v. Modern Enterprise Solutions, Inc., Timothy Durant, and Andrew Uzpen, (MN Dist. Ct., 4th Dist. (Hennepin Co.) No. 27-CV-15-17171)
- Golden Supply, Inc., a Minnesota Corporation v. Jeffrey Hunt and Ken Aronckes, (MN Dist. Ct. 4th Dist. (Hennepin Co.) No. 27-CV-15-1625)
- Jerry Wilkinson and Karen Wilkinson v. State Farm Fire and Casualty Company, (U.S. Dist. Ct. E.D. Wis.) Case No. 14 CV 1187)
- Greiner Construction, Inc. vs. Bert Westerman et al., (MN Dist. Ct., 4th Dist. (Hennepin Co.)
- Samantha Orduno, et. al. v. Richard Pietrzak, et al. (United States District Court (Dist. of MN) No. 0:14-cv-01393-ADM-JSM)
- Zimmer, Inc. v. Stryker Corporation; Howmedica Osteonics Corp. d/b/a Stryker Orthopedics; and Cody Stovall. (United States District Court (Northern District of Indiana of Indiana South Bend Division) Case No. 3:14-cv-00152-JD-Can)
- Robert Half International Inc., v. Donna Farrugia, et al. (Superior court of State of California (San Francisco Co.) No. CGC-14-539338)
- Emergent Systems Exchange, LLC, vs. Daniel Ray McGinnis, et al., (MN Dist. Ct., 4th Dist. (Hennepin Co.) No. 27-CV-147338)
- Tristan Connor Damron v. John E. Norris, et. al., (Ala. Circuit Court (Elmore Co.) No. CV11-900259.00)
- Curtis Trude, et al. v. Glenwood State Bank, et al. (MN Dist. Ct., 8th Dist. (Meeke Co.) No. 47-CV-12-176)
- Pioneer Home, Inc. v. American Federal Bank, (MN Dist. Ct., 7th Dist. (Hennepin Co.) No. 56-CV-13-3353)
- Prosthetic Laboratories of Rochester, Inc., v. Brandon Sampson, et al., (MN Dist. Ct. 3rd Dist. (Hennepin Co.) No. 55-CV-133625)
- Jenine Ellison v. Advanced Surgery Center of Palm Beach Count, LLC, (15th Circuit Court (Palm Beach County), Florida. No: 502011CA020861XXXXMB.)
- JIT Companies, Inc. v. Erik Edwin Swanson, (MN Dist. Ct., 3rd Dist. (Hennepin Co.) No. 66-CV-132532)



Publications List – Mark Lanterman

Bench & Bar of Minnesota

How to avoid an old scam with a new twist, November 2020

Your back-to-school tech brush-up, October 2020

The Twitter breach and the dangers of social engineering, September 2020

Cyber risk: Is your data retention policy helping or hurting?, August 2020

Cyber riots and hacktivism, July 2020

Ethical considerations of working from home: Protecting client data, May 2020

Cybersecurity in pandemic times, April 2020

Business continuity and coronavirus planning, March 2020

Doxxing made easy: social media, March 2020

Taking responsibility for your cybersecurity, February 2020

Beyond compliance: Effective security training, January 2020

Doxxing redux: The trouble with opting out, December 2019

Proportionality and digital evidence, November 2019

AI and its impact on law firm cybersecurity, October 2019

Too secure? Encryption and law enforcement, September 2019

Security, Convenience and Medical Devices, August 2019

Physical Security as Part of an Incident Response Plan, July 2019

Papers and Effects Part II, May/June 2019

Security Considerations for Law Firm Data Governance, March 2019

The Marriott breach: four years?, February 2019

"Papers and effects" in a digital age, co-authored with Judge (Ret.) Rosenbaum, January 2019

The Chinese spy chip scandal and supply chain security, December 2018.
(Republished in *The Computer & Internet Lawyer*)

Don't forget the inside threat, November 2018

Cyberattacks and the costs of reputational harm, October 2018

Fair elections and cybersecurity, September 2018

E-discovery vs. forensics: Analyzing digital evidence, August 2018

Social media and managing reputational risk, July 2018

Managing Cyber Risk: Is cyber liability insurance important for law firms?, June 2018. (Republished in *The Computer & Internet Lawyer*)

Social engineering: How cybercriminals capitalize on urgency, April 2018

Stephen Allwine: When crime tries to cover its digital tracks, March 2018

Is the Internet of Things spying on you?, February 2018

#UberFail, January 2018

Ransomware: To pay or not to pay?, December 2017

How digital evidence supported gerrymandering claims, November 2017

Facial recognition technology brings security & privacy concerns, October 2017

Putting communication and clients first in digital forensic analysis, September 2017

Digital evidence: New authentication standards coming, July 2017

Your Personal Data – Or is it? Doxxing and online information resellers pose threats to the legal community, June 2017

What You Don't Know Can Hurt You: Computer Security for Lawyers, March 2014

Minnesota Lawyer

Phishing, vishing and smishing – oh, my!, January 2018

Equifax was unprepared for a data breach, September 2017

Cybersecurity and forensic application in cars, July 2017

Preventing 'spear-phishing' cyber attacks, May 2017

Opting out when private information goes public, March 2017

Are fingerprints keys or combinations?, February 2017

Digital Forensics and its role in data protection, February 2017

Acknowledge the security issues, December 2016

Modern life is driven by the internet of things, November 2016

Are medical devices vulnerable to hackers?, October 2016

Digital evidence as today's DNA, September 2016

Colorado Lawyer

Is Emailing Confidential Information a Safe Practice for Attorneys?, July 2018.
(Republished in The Journals & Law Reviews database on WESTLAW)

International Risk Management Institute, Inc. (IRMI)

Security from Home: Continuing to Work and Learn Amid COVID-19, September 2020

Operational Risk Revisted in the Wake of COVID-19, June 2020

Cyber Threats and Accounting for Operational Risk, March 2020

Human Aspect of Incident Response Investigations, January 2020

The Impact of Digital Incompetency on Cyber-Security Initiatives, September 2019

Communication in Responding to Cyber Attacks and Data Breaches, June 2019

Cyber Security and Resilience, January 2019

Leadership in Developing Cultures of Security, September 2018

Real-Life Consequences in a Digital World: The Role of Social Media, July 2018

Some Thoughts on the Dark Web—and How it Affects You, March 2018

Personal Information and Social Media: What Now to Post, September 2017

Managing Doxxing-Related Cyber Threats, July 2017

Understand the Layers of Cyber-Security and What Data Needs Protecting, March 2017

Learn about the Internet of Things: Connectivity, Data, and Privacy, January 2017

Assessing Risk and Cyber-Security, September 2016

SCCE The Compliance & Ethics Blog

The Components of Strong Cybersecurity Plans: Parts 1-5, 2017

Prevention Is the Best Medicine, August 2016

Lawyerist

Detection: The Middle Layer of Cybersecurity, April 2017

Don't Be Too Hasty! What to Do When an Email Prompts You to Act Quickly,
February 2017

How to Avoid Spoofing, Spear Phishing, and Social Engineering Attacks, October
2016

Law Practice

The Dark Web, Cybersecurity and the Legal Community, July/August 2020

Captive International

COVID-19 and the importance of the cyber captive, April 2020

Attorney at Law Magazine

The Digital Challenges of COVID-19, June 2020

E-Discovery Deskbook

Chapter Thirteen "Forensic Experts—When and How to Leverage the Talent" co-authored with John M. Degan Briggs and Morgan, P.A.