Thomas H. Bienert, Jr. (CA State Bar No. 135311, *admitted pro hac vice*)
tbienert@bmkattorneys.com
Whitney Z. Bernstein (CA State Bar No. 304917, *admitted pro hac vice*)
wbernstein@bmkattorneys.com
BIENERT KATZMAN, PLC
903 Calle Amanecer, Suite 350
San Clemente, CA 92673
Telephone: (949) 369-3700
Facsimile: (949) 369-3701

Attorneys for James Larkin

Gary S. Lincenberg (CA State Bar No. 123058, *admitted pro hac vice*)
glincenberg@birdmarella.com
Ariel A. Neuman (CA State Bar. No. 241594, *admitted pro hac vice*)
aneuman@birdmarella.com
Gopi K. Panchapakesan (CA State Bar No. 279586, *admitted pro hac vice*)
gpanchapakesan@birdmarella.com
BIRD, MARELLA, BOXER, WOLPERT, NESSIM,
DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

Attorneys for John Brunst

Additional counsel listed on following page

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

United States of America,

Plaintiff,

vs.

Michael Lacey, *et al.*,

Defendants.

CASE NO. 2:18-cr-00422-SMR

DEFENDANTS' RESPONSE TO THE UNITED STATES' PRE-HEARING MEMORANDUM REGARDING DEFENDANTS MOTION TO COMPEL (Doc. 759) AND SUPPLEMENTAL AUTHORITIES

Paul J. Cambria, Jr. (NY State Bar No. 1430909, *admitted pro hac vice*)
pcambria@lglaw.com
Erin E. McCampbell (NY State Bar No. 4480166, *admitted pro hac vice*)
emccampbell@lglaw.com
LIPSITZ GREEN SCIME CAMBRIA LLP
42 Delaware Avenue, Suite #120
Buffalo, NY 14202
Telephone: (716) 849-1333
Facsimile: (716) 855-1580

Attorneys for Michael Lacey

Bruce Feder (AZ State Bar No. 004832)
bf@federlawpa.com
FEDER LAW OFFICE, P.A.
2930 E. Camelback Road, Suite 160
Phoenix, AZ 85016
Telephone: (602) 257-0135
Facsimile: (602) 954-8737

Attorneys for Scott Spear

David Eisenberg (AZ State Bar No. 017218)
david@deisenbergplc.com
DAVID EISENBERG, P.L.C.
3550 N. Central Avenue, Ste. 1550
Phoenix, Arizona 85012
Arizona State Bar No. 017218
Telephone: (602) 237-5076

Attorneys for Andrew Padilla

Additional counsel listed on following page

Joy Bertrand (AZ State Bar No. 024181)
joyous@mailbag.com
JOY BERTRAND, ESQ.
PO Box 2734
Scottsdale, Arizona 85252-2734
Telephone: (602) 374-5321
Fax: (480) 361-4694

Attorneys for Joye Vaught

Before the commencement of the evidentiary hearing on Defendants' Motion to Compel Discovery (Doc. 649, the "Motion"), the United States filed a fifteen-page memorandum setting forth what it expected the evidence to show and making additional argument in opposition to the Motion. Defendants submit this response, which distills the actual testimony (spanning 444 pages, to date) into a more manageable size. As the Court said it did not wish to receive further argument, this response a) focuses almost exclusively on the testimony of the government's agents and witnesses and b) sets forth the pertinent testimony without argument.[1] Following the distillation of the testimony, Defendants have cited supplemental authorities regarding the "reasonably usable" standard and degradation of electronically stored evidence.

1. **Backpage's I.T Systems Were Fully Functional Before the Government's Seized Them**

   - The Backpage I.T. systems were "working and functioning" when the government seized them [Gerken, Tr., 88/14-24].

2. **The Government Seized and Disassembled Backpage's I.T. Systems, Making No Effort to Preserve Their Functionality**

   - Agent Cullen, who was on the government's seizure team, testified that the government was "there to power down the servers and take them back to Phoenix" [Cullen, Tr., 17/15-17] and he did not "know the reason" why the government did not "leave the servers up and running" [Cullen, Tr., 25/13-16].
   - Agent Cullen "did not" ask Will Gerken for a "schematic of the servers and their configuration so that the servers could be reconfigured and operate in their normal functional way" [Cullen, Tr., 39/10-14].

[1] Due to the amount of testimony, the technical nature of the issues and the testimony, and the fact that Defendants did not know many of the facts adduced during the hearing when they filed their Motion or their reply in support of the Motion, Defendants believe that further briefing or argument would be appropriate.

- Agent Cullen admitted it "would have been easy enough to ask Mr. Gerken" for the information needed to keep the servers functional, like IP addresses, but the government "chose not to" [Cullen, Tr., 48/12-25] and also made "no effort to identify [the] different roles of the servers" [Cullen, Tr., 51/22-25] or "the interrelationship of the various system components" [Cullen, Tr. 51/3-9].[2]
- Agent Cullen admitted the government "took no steps with Gerken to try to fill in all of the things . . . necessary to reassemble [the servers in their] original evidentiary form" [Cullen, Tr., 45/1-5].
- Agent Robinson, who also was on the government's seizure team, admitted that the government did not "note which wires were connected to what" [Robinson, Tr., 355/25 - 356/5].
- Despite several calls by the defense for access to "a functioning Backpage system," Agent Robison did not "reach[] out to Mr. Gerken to try to figure out how this system worked and whether it could be resurrected until May of this year," after the Court "told the government she wanted a status of the server system" [Robinson, Tr, 357/10 - 358/1].

3. The Government Knew Backpage's I.T. Systems Contained Information Relevant to the Defense—Including Exculpatory Information

- Agent Robinson admitted that the Backpage I.T systems would have information "relevant to someone investigating the degree to which Backpage knew a particular ad or advertiser was acting illegally" [Robinson, Tr., 348/7-21].

[2] The government now claims it would be "a difficult, technologically challenging task" to reassemble the website because "the IP (Internet Protocol) addresses of the different servers as they were configured at that time would need to be rediscovered, and the organization and interrelationship of the various system components would need to be reconstructed" [United States' Pre-Hearing Memorandum Regarding Defendants' Motion to Compel, Doc. 759, pp. 7-8]—in other words, due to the lack of the information the government "chose not to" obtain when it seized the servers.

- Agent Robinson acknowledged he "knew that the [Backpage I.T.] system would have information relating to Backpage trying to help stop underage sex" (*e.g.*, reports to NCMEC) [Robinson, Tr., 342/25 – 343/8].

4. The Government Had Several Options for Seizing the Backpage I.T. Systems and Taking Them Offline Without Destroying Their Functionality

A. The Government Could Have Had Mr. Gerken Disconnect Backpage's I.T. Systems from the Internet and Put the Systems into Read-Only Mode

- The Backpage servers in Tucson were in a "closed facility" and were "in a cage area that's locked inside the locked building" [Robinson, Tr., 353/11-20].
- The government could have "take[n] the Backpage system off line, secure[d] it, lock[ed] it up in the place where it was and work[ed] on it and use[d] it in a read only capacity for some period of time as of April 6 going forward" [Gerken, Tr., 97/18-24].
- "Disconnect[ing] the Web site from the internet such that the public could no longer access it" would have been "very easy" [Gerken, Tr., 129/14-22].
- Putting the Backpage systems into read only mode would have frozen "the data in time exactly as it existed the moment you put it into read only mode" [Gerken, Tr., 149/12-16] and "would also have maintained the administrative functionality that the defendants have been asking for" [Loehrs, Tr., 383/21 – 384/12].
- Agent Frost admitted there was no reason the "Tucson servers could not have been taken off line and accessed through encrypted channels remotely" [Frost, Tr., 228/1-4].
- Before the Backpage I.T. systems were disassembled, Gerken could have "create[d] a read only version" of the system in "a day or two" and could have made two separate read only versions of the system in "about two weeks" [Gerken, Tr., 127/19 - 128/19]. The cost to do so would have been "significantly less than [his] estimate now" [Gerken, Tr., 128/20-23].

B. The Government Could Have Imaged Backpage's I.T. Systems and Left Them Intact

- Agent Frost was "aware that the government has in other cases left servers and databases intact, imaged them on site, and gone away and thereby not destroyed the data" [Frost, Tr., 300/12-17].
- In particular, Agent Frost was familiar with the MegaUpload case, which involved "over 1,100 servers," and in which "the government did not seize any of the upload servers, instead copied certain data from the servers and essentially took them offline while the government was there so they could be imaged, but then left the servers on the premises" [Frost, Tr., 300/18 – 301/4].
- Agent Cullen also acknowledged government could have "made a mirror image of these [servers] and left them there intact" [Cullen, Tr., 39/25-40/3].

C. The Government Could Have Collected the Information Needed to Move and then Restore Backpage's I.T. System, Before Disassembling the System

- The government could have "take[n] the Backpage system that was at Login hosted by DesesrtNet," "shut it down and move[d] it to a different location," and "do[ne] it in a way so that when you get to the different location" it would "all work the same way;" Gerken had done just that with the Backpage I.T. systems "not long before the day of the search" [Gerken, Tr., 94/14-95/9].

D. Because of the Redundancy of Backpage's I.T. Systems, the Government Could Have Left One of the Many Redundant Systems Intact

- Will Gerken was the "lead developer" of Backpage.com and no one was "better equipped to answer questions about how the Web site was managed" [Gerken, Tr., 59/20 – 60/14].
- Mr. Gerken testified that the Backpage I.T. systems in Tucson included a master ad database server and three replicated ad database servers, each containing "all the same information" and each being "redundant" [Gerken, Tr., 61/24 – 62/25], as well as three "completely redundant" image servers [Gerken, Tr., 63/10-16].

- Mr. Gerken also testified that, "in terms of actual data, as long as you had the master database server, you wouldn't need the replicated servers because it's all the same information . . . They're redundant" [Gerken, Tr., 62/22-25].
- Not only did the Backpage I.T. systems in Tucson have redundancy, the Backpage I.T. systems in Amsterdam and Tucson were designed to be "fail over site[s]," where either could run the website independent of the other [Gerken, Tr., 65/6-20]. The Tucson and Amsterdam sites were "duplicate sites" [Frost, Tr., 279/1-4].
- And, like in Tucson, the Backpage I.T. systems in Amsterdam had master ad and image servers and redundant replicated ad and image servers [Gerken, Tr., 65/21 - 66/5].

E. The Government Had a Second Chance with Backpage's Amsterdam System, But Failed to Document the Configuration of that System so It Could be Moved and Reassembled

- After being "overwhelmed with the number of servers" seized from Tucson and learning there were "two copies of the data," one in Tucson and one in Amsterdam, Agent Frost "made plan[s] . . . to go to Amsterdam. . . and isolate those servers from the Internet so they could be left exactly how they were intact" so they could be "remotely accessed by the FBI from the United States" [Frost, Tr., 155/19 – 156/10].
- Frost wanted to access the still-functioning Amsterdam servers because "the Tucson servers were so voluminous and difficult to put back together and assemble" and were a "large puzzle" [Frost, Tr., 279/12-19].
- The Tucson servers were "a big puzzle" "because … the IP addresses of the different servers had not been retained and the organization and interrelationship of the system components had not been retained" [Frost, Tr., 299/19 – 300/4].
- Frost tried to "virtualize those puzzle pieces to bring Backpage into a functioning environment," but was not able to do so [Frost, 279/20-23; 233/19 – 234/15].

- Frost "realized it would be much easier to be able to access the servers live and just look at everything up and running" and it "would have been much easier than dead box forensics" [Frost, Tr., 227/20-25].
- Because the Dutch National Police would not "allow the servers to stay in Amsterdam live," Agent Frost "identif[ied] nine servers for the Dutch to seize," which the Dutch police then seized [Frost, Tr., 157/7 – 158/18].
- Agent Frost picked those nine servers by "logg[ing] in" to various servers "to verify ... what was contained in those servers" [Frost, Tr., 280/23 – 281/5].
- Agent Frost did not, however, "record the different IP addresses that were assigned to the different servers" or "note the interrelationships of the various system components" in the Amsterdam system [Frost, Tr., 281/13-20]—the same failure he testified was responsible for the "big puzzle" with the Tucson servers.

5. The Government's "Two Server" Extracted Data Seriously Degrades the Defense's Ability to Access Ad Data, Does Not Allow for the Viewing of Ads, and Provides No Access to Most Payment Data

Ad Data

- The Backpage ad data was split between "geographically divided" "market databases" and a "central" database, which contained "a subset of the ad across all of those market databases;" "the market databases are really where you want to get the ad content from;" "the central one is telling you where they are" [Gerken, Tr. 70/2-25].
- There were "over a hundred" market databases [Frost, Tr., 244/1-2] and the data for each market database was held in numerous separate database "tables" [Frost, Tr.180/23 – 181/12]. Agent Frost's PowerPoint identified more than 100 separate tables just for the Phoenix market [Exh. 9, pp. 5-8] (suggesting more than 10,000 tables to search for all markets).
- During "the time of the 50 ads in the indictment," just "the six years from 2013 to 2018," "many, many millions" of ads ran on Backpage [Robinson, Tr., 339/16 – 339/21]. Agent's Frost's PowerPoint demonstrates that many of the individual

tables for the Phoenix marketplace have hundreds of thousands of rows and several have millions of rows. [Exh. 9, pp. 5-8, column 2.]. The government contends the defense should "run[] manual queries" on these thousands of tables with hundreds of thousands or millions of rows [Gerkin, Tr., 145/8-10], with some of those tables having "91 total fields" [columns] "that wouldn't fit across the screen." [Frost, Tr., 182/17-25].

- Even with access to the thousands of database tables extracted from the Backpage I.T. systems, a person cannot access ad data without being "proficient in working in SQL" [Gerken, Tr., 83/13-18] and without being "familiar with the databases and how it stores data to piece it all back together" [Frost, Tr., 188/9-14].
- In contrast, when the Backpage I.T. systems were functioning, a person could access ad data through the "object editor" without knowing SQL; even a lawyer could do it [Gerken, Tr., 131/4-16].
- Although the underlying data from the ad database may be available in the thousands of tables extracted from the Backpage I.T. systems, the functioning system was "more easily searchable and manipulable . . . for a non-expert" and, importantly, the underlying data cannot now be displayed "in the format that they looked like" when the website was operational [Gerken, Tr., 138/5 - 139/1].
- Because the data extracted from the tables does not resemble an ad on Backpage, Agent Frost manually created a facsimile of an ad on Backpage for a case in New York, by "assembl[ing] the data extracted from the database and put[ting] it in a format where the information that would have appeared on the ad was in one location with the images, the title, the header, the advertisement, phone number, posting ID" [Frost, Tr., 276/22 – 277/5]—proving the point that extracted data is not a substitute for an ad in the format it would have appeared on Backpage.[3]

[3] That Agent Frost was able to make a collage approximating the look of a Backpage ad from data and images he manually extracted from the tables does not mean that the defense should

- Mr. Gerken admitted "if the government has an expert who says, I looked at all these ads and they were all obviously for prostitution," the defense would not be able to "challenge that expert by showing her ads from the actual Web site" using the "two server" extracted data [Gerken, Tr., 139/18-25].[4]
- Agent Frost admitted the defense could no longer "look at a report with a check box [to determine if an ad] was reported to NCMEC," but would either have to "look up fields of syntax and run code and create a Mint HeidiSQL database to do that" or "hire an expert to do that" [Frost, Tr., 244/5-23].

Payment Data

- A significant part of "this case is about money, how money was paid and what was done with that money" [Robinson, Tr., 351/12-15].
- The Backpage I.T. systems were configured to "allow someone working at Backpage to access, not just ad, photo, and text information, but payment information" [Gerken, Tr., 106/10-22].
- The Amsterdam site contained Backpage's credit card processing system, referred to as the "payment processing island" or "PPI" [Gerken, Tr., 66/14-25].
- The "DesertNet managed Backpage [ad] database" contained only "some very basic rudimentary [payment] information, such as a real generic invoice just for statistic [sic] purposes," but "accounting information would be on the PPI" [Gerken, Tr., 68/12-20].
- The ad data the government extracted from the Backpage I.T. systems "is not connected . . . to the . . . payment processing island system" and "it's not possible .

dust off their collage-making skills, as that case involved one ad (or a handful ads) and, here, the government puts at issue millions of ads: "virtually every dollar flowing into Backpage's coffers represent[ed] the proceeds of illegal activity" [Robinson, Tr., 347/5-8].

[4] This issue is not just theoretical, as the government has listed as potential witnesses at least one, and likely many, witnesses who would testify (if permitted by the Court) that they had reviewed large numbers of ads on Backpage and concluded that many or all related to prostitution.

. . to link an ad to the method of payment without going through a number of complicated steps" [Frost, Tr., 308/12 – 309/19].

- Even though the rudimentary payment data previously available in the "object editor" view may exist in the thousands of database tables the government extracted, the "invoice data may be stored in different tables in the database, potentially even in different databases," while, before the seizures, the "object editor" "pulled together all of those pieces to provide a representation of all the invoice data" [Gerken, Tr., 142/9 – 143/1].

6. Resolution of Certain Issues Relating to Accessing Hard Disks and Forensic Images

Since the last hearing on October 25, 2019, Defendants and the government have met and conferred about the defense expert's inability to access certain hard disks produced by the government and her inability to access the forensic images on other disks. The parties will provide further information to the Court at the upcoming hearing, but, briefly:

a) The government has acknowledged that several of the hard disks it provided have physical defects rendering them unreadable; the government will replace those hard disks with new disks containing the data on the originals.

b) The government provided additional information about the manner in which it created the hard disks, which the defense expert believes will allow her to access the forensic images on the disks without physical defects.

Defendants' Motion was not premised on an inability to access the hard disks or the forensic images on them, but on a lack of access to functional I.T. systems. Even assuming a) and b) lead to the defense expert being able to access and restore the forensic images, that will not lead to Defendants having access to functional I.T. systems. At most it would address an ancillary issue raised in the reply.

Conclusion

When the government seized the Backpage I.T. systems, they were fully functional and allowed persons without technical skills to readily search and extract large amounts of data

from both the ad database and from the payment processing system.[5] Because the government failed to take *any* steps (much less reasonable steps) to preserve the functioning of those I.T. systems (as opposed to merely protecting raw data on the hard disks in them), the systems now can be searched only by I.T. experts and, even then, only by cumbersome manual searches producing data that is not readily usable. The Motion did not ask the Court to compel the government to create something that did not exist when the government seized it from a third party. To the contrary, the Motion asked the Court to "compel the government to provide Defendants access to Backpage's systems, servers, databases and data, with the same functionality and in the same condition as they existed at the time of their seizure, or, alternatively, in a format wherein the government restores the systems, servers, databases, and data so they are searchable and viewable as they existed at the time of the government's seizures." [Motion, p. 17]. To that end, Defendants request that the Court compel the government to restore one copy of the Backpage ad database, payment processing system, and other systems to a "read only" state so they are searchable and viewable as they existed at the time of the government's seizures.

Glossary

FreeBSD: An open source operating system used to power modern servers with advanced networking, security, and storage features.

SQL: A language used in programming and designed for managing data held in a relational database management system.

MySQL: An open-source relational database management system.

MariaDB: An open-source, commercially supported fork of the MySQL relational database management system.

HeidiSQL: An open-source administration tool for MySQL

ZFS: A combined file system and logical volume manager.

[5] They also allowed access to information on Backpage's cooperation with law enforcement. Agent Frost "asked Mr. Gerken which server" the "information that Backpage regularly and voluntarily provided in response to law enforcement subpoenas" was on, but Agent Frost did not "forensically image that server" [Frost, Tr., 297/25 – 298/10] and it appears the government has not produced that information.

SUPPLEMENTAL AUTHORITIES

1. **In Defendants' Reply in Support of Motion to Compel Discovery (Doc. 717), pp. 4 – 5, Defendants argued that the government has failed to provide discovery in a "reasonably usable form," as required by the Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases" (the "ESI Protocol"). The following decisions interpret the "reasonably usable form" requirement under Fed. R. Civ. P. 34(b)(2)(E)(ii) and provide guidance for the interpretation of that same term under the ESI Protocol:**

Jannx Medical Systems, Inc. v. Methodist Hospitals, Inc., **2010 WL 4789275 (U.S.D.C. N.D. Ind. Nov. 17, 2010)** (rejecting plaintiff's "production of electronic database data in .pdf form" and granting "Defendants' Motion to Compel to the extent that Defendants request that Plaintiff produce responsive information in an electronic database format that allows the information to be reasonably usable, *i.e.,* fully searchable and manipulable, with the connections between data fields intact.")

Dekeyser v. Thyssenkrupp Waupaca, Inc., **2015 WL 10937559 (U.S.D.C. E.D. Wisc. April 10, 2015)** (ordering defendant to "produce all data and information maintained in its databases . . . in an electronic, organized and usable format," stating "I agree with Plaintiffs that, unless there is undue burden . . . they should be able to not only use the MSDSs but use and search the database with roughly the same ease and efficiency as can Waupaca and its employees. Although a party generally should not be required to overhaul and reformat its own data, the Committee Notes to Rule 34 cited by both parties make clear that a party also cannot produce information in a manner that degrades searchability: '[T]he option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in litigation. If the responding party ordinarily maintains information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.' Adv. Comm. Notes to 2006 amendment to Rule 34(b).")

***Craig & Landreth, Inc. v. Mazda Motor of America, Inc.*, 2009 WL 2245108 (S.D. Ind. July 27, 2009)** ("[D]efendant maintains that 'when it produced many documents in portable document format ('PDF'),' it was well within the requirements of the Federal Rules of Civil Procedure because it produced all of the requested documents in a 'reasonably usable form.' The Magistrate Judge disagrees. Plaintiffs' requests clearly indicate to this court that they were seeking electronically stored information that consisted of searchable databases of Mazda vehicles, and not simply a list of vehicles in PDF format. Even if plaintiffs' requests were not as articulate as they could have been in order to put defendant on notice of the format of the information sought, the Advisory Committee Note to Rule 34 is clear. Defendant was not permitted to convert any of its electronically stored information to a different format that would make it more difficult or burdensome for plaintiffs to use.")

***Mills v. Billington*, 2013 WL 12312811 (U.S.D.C. D.C. May 23, 2013)** (rejecting the production of documents in paper format and ordering their production in a reasonably usable electronic form, citing the Advisory Committee Notes to Fed. R. Civ. Pro. 34; "Though outside the scope of the current discovery proceedings, Defendant should be aware that courts have found the conversion of data to an inaccessible format to be sanctionable. *See Treppel v. Biovail Corp.*, 233 F.R.D. 363, 372, n.4 (S.D.N.Y. 2006) "permitting the downgrading of data to a less accessible form—which systematically hinders future discovery by making the recovery of the information more costly and burdensome—is a violation of the preservation obligation.")

***Treppel v. Biovail Corp.*, 233 F.R.D. 363, 372 n.4 (S.D.N.Y 2006)** ("The Second Circuit has held that conduct that hinders access to relevant information is sanctionable, even if it does not result in the loss or destruction of evidence. *See Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99, 110 (2d Cir.2002). Accordingly, permitting the downgrading of data to a less accessible form—which systematically hinders future discovery by making the recovery of the information more costly and burdensome—is a violation of the preservation obligation.")

2. **Even before the adoption of the ESI Protocol and its "reasonably usable form" requirement in 2012, district courts looked to Fed. R. Civ. P. 34 for guidance on the government's obligations to produce ESI under Fed. R. Crim. P. 16:** ***United States v. Briggs*****, 2011 WL 4017886, *8 (W.D.N.Y. Sept. 8, 2011)** (pursuant to Fed. R. Crim. Pro. 16(d) and its inherent authority, district court applied "reasonably usable form" standard from Fed. R. Civ. Pro. 34(b)(2)(E)(ii) to government's production of ESI in a criminal case)

U.S. v. O'Keefe**, 537 F.Supp.2d 14 (D.D.C. 2008)** (district court looked to Fed. R. Civ. Pro. 34(b)(2)(E)(ii) to assess the government's production of ESI, noting the "Federal Rules of Civil Procedure in their present form are the product of nearly 70 years of use and have been consistently amended by advisory committees consisting of judges, practitioners, and distinguished academics to meet perceived deficiencies. It is foolish to disregard them merely because this is a criminal case, particularly where, as is the case here, it is far better to use these rules than to reinvent the wheel when the production of documents in criminal and civil cases raises the same problems.")

DATED: November 26, 2019

Thomas H. Bienert, Jr.
Whitney Z. Bernstein
BIENERT KATZMAN, PLC

By: */s/ Thomas H. Bienert, Jr.*
Thomas H. Bienert, Jr.
Whitney Z. Bernstein
Attorneys for James Larkin

DATED: November 26, 2019

Paul J. Cambria, Jr.
Erin E. McCampbell
LIPSITZ GREEN SCIME CAMBRIA LLP

By: */s/ Paul J. Cambria, Jr.*
Paul J. Cambria, Jr.
Attorneys for Michael Lacey

DATED: November 26, 2019

Bruce Feder
FEDER LAW OFFICE, P.A.

By: */s/ Bruce Feder*
Bruce Feder
Attorneys for Scott Spear

DATED: November 26, 2019

Gary S. Lincenberg
Ariel A. Neuman
Gopi K. Panchapakesan
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.

By: */s/ Ariel A. Neuman*
Ariel A. Neuman
Attorneys for John Brunst

DATED: November 26, 2019

David Eisenberg
DAVID EISENBERG, P.L.C.

By: */s/ David Eisenberg*
David Eisenberg
Attorneys for Andrew Padilla

DATED: November 26, 2019

Joy Bertrand
JOY BERTRAND, ESQ.

By: */s/ Joy Bertrand*
Joy Bertrand
Attorneys for Joye Vaught

CERTIFICATE OF SERVICE

I certify that on this 26th day of November 2019, I electronically transmitted a PDF version of this document to the Clerk of the Court, using the CM/ECF System, for filing and for transmittal of a Notice of Electronic Filing to the following CM/ECF registrants listed below.

/s/ Toni Thomas
Toni Thomas

Anne Michelle Chapman, anne@mscclaw.com
Erin E. McCampbell, emccampbell@lglaw.com
Anthony R. Bisconti, tbisconti@bienertkatzman.com
Ariel A. Neuman, aan@birdmarella.com
Bruce S. Feder, bf@federlawpa.com
James C. Grant, jimgrant@dwt.com
Lee David Stein, lee@mscclaw.com
Paul J. Cambria, pcambria@lglaw.com
Robert Corn-Revere, bobcornever@dwt.com
Ronald Gary London, ronnielondon@dwt.com
Janey Henze Cook, janey@henzecookmurphy.com
John Lewis Littrell, jlittrell@bmkattorneys.com
Thomas H. Bienert, Jr. tbienert@bienertkatzman.com
Whitney Z. Bernstein, wbernstein@bienertkatzman.com
Gary S. Lincenberg, glincenberg@birdmarella.com
Gopi K. Panchapakesan, gpanchapakesan@birdmarella.com
Michael D. Kimerer, mdk@kimerer.com
Rhonda Elaine Neff, rneff@kimerer.com
David S. Eisenberg, david@deisenbergplc.com
Joy Malby Bertrand, joyous@mailbag.com
John Jacob Kucera, john.kucera@usdoj.gov
Kevin M. Rapp, Kevin.Rapp@usdoj.com
Margaret Wu Perlmeter, Margaret.perlmeter@usdoj.gov
Reginald E. Jones, reginald.jones4@usdoj.gov
Peter Shawn Kozinets, Peter.Kozinets@usdoj.gov
Andrew C. Stone, andrew.stone@usdoj.gov