COMMONWEALTH OF MASSACHUSETTS

WORCESTER, ss.

SUPREME JUDICIAL COURT
No.

APPEALS COURT
No. 2026-P-0295

COMMONWEALTH

v.

MICHAEL MORIN

# DEFENDANT'S APPLICATION FOR DIRECT APPELLATE REVIEW OF THE ORDERS OF THE WESTBOROUGH DISTRICT COURT

Nicholas Matteson
BBO # 688410
Law Office of Nicholas Matteson
P.O. Box 2633
Holyoke, MA 01041
(857) 415-1608
nm@mattesonlawoffice.com

## TABLE OF CONTENTS

REQUEST FOR DIRECT APPELLATE REVIEW ..... 3

PRIOR PROCEEDINGS ..... 4

STATEMENT OF RELEVANT FACTS ..... 5

ISSUE PRESENTED ..... 7

ARGUMENT ..... 8

**The delay of more than ten months before seeking a search warrant after reported uploads of child pornography resulted in the search warrant application failing to establish probable cause that the target of the warrant or any electronic devices he controlled would be found in the residence to be searched.** ..... 8

REASONS WHY DIRECT APPELLATE REVIEW IS APPROPRIATE ..... 17

CONCLUSION ..... 18

CERTIFICATE OF COMPLIANCE ..... 19

CERTIFICATE OF SERVICE ..... 20

DOCKET ENTRIES ..... 21

ORDER ON MOTION TO SUPPRESS ..... 25

TYPED VERSION OF HANDWRITTEN ENDORSEMENT ON MOTION TO SUPPRESS ..... 26

APPLICATION FOR SEARCH WARRANT ..... 27

## REQUEST FOR DIRECT APPELLATE REVIEW

"Every investigation, including the possession and distribution of child pornography, has a shelf life." Commonwealth v. Guastucci, 486 Mass. 22, 30 (2020). This appeal concerns a delay of more than ten months between reported uploads of child pornography and the application for a search warrant—well beyond the seven-month delay addressed in Commonwealth v. Guastucci, 486 Mass. 22, 27 (2020)—and whether this significantly longer delay exceeded the shelf life of the investigation and rendered the information supporting the warrant stale.

The defendant challenged the probable cause finding in a motion to suppress, arguing that the information supporting the warrant was stale. The motion judge found the delay not to be unconstitutional, citing Guastucci, 486 Mass. at 27, but without any analysis of how the significantly longer period between the uploads and the application for the warrant affected the probable cause analysis.

Pursuant to Mass. R.A.P. 11, the defendant, Michael Morin, now requests that this Court allow direct appellate review to provide guidance to lower courts on the proper analysis in addressing a claim of

staleness where the delay in seeking a search warrant stretches substantially beyond that addressed in Guastucci, 486 Mass. at 27.

## PRIOR PROCEEDINGS

On December 11, 2023, the defendant, Michael Morin, was arraigned in the Westborough Division of the District Court on one count of possession of child pornography. Mr. Morin filed a motion to suppress the fruits of a search warrant, arguing that the warrant application failed to establish probable cause. After a non-evidentiary hearing, the motion judge denied the motion in a handwritten endorsement on August 12, 2025.

Thereafter, Mr. Morin tendered a guilty plea reserving his right to appeal the order denying his motion to suppress. On December 11, 2025, the court accepted the tender and sentenced Mr. Morin to probation supervision for a term of two years. On December 18, 2025, Mr. Morin timely noticed his appeal of the order denying his motion to suppress.

## STATEMENT OF RELEVANT FACTS

On November 13, 2021, a user of Snapchat—a mobile application that allows users to share photographs, video recordings, and chats—uploaded nine files that Snapchat identified as potential child pornography. On the following day, November 14, 2021, Snapchat reported the uploads to the CyberTipline of the National Center for Missing and Exploited Children. On December 21, 2021, the CyberTipline report was made available to the Massachusetts State Police. On December 23, 2021, an administrative subpoena was issued to Verizon, the internet service provider associated with the IP address of the Snapchat user. In response, Verizon provided subscriber information related to that IP address, identifying the subscriber as Linda Carpenter of 31 Harvard Avenue in Shrewsbury. The Verizon response also included a phone number and a specific model of Motorola cellular phone that were associated with the uploads. On February 22, 2022, the CyberTipline report was forwarded to Sergeant David Faucher of the Shrewsbury Police Department.

On May 9, 2022, Sergeant Faucher "ran a registry check" on the Harvard Avenue address. The check "revealed" three names: Linda

Carpenter, Mr. Morin, and Kristina Sarin, with a driver's license number for each. Sergeant Faucher also checked Town of Shrewsbury records and determined 31 Harvard Avenue to be co-owned by Sajiv Sarin and Linda Carpenter. Sergeant Faucher conducted a LexisNexis inquiry of the phone number provided by Verizon. That inquiry revealed an "attached individual" of Mr. Morin of 31 Harvard Avenue in Shrewsbury.

On May 11, 2022, Sergeant Faucher conducted surveillance on 31 Harvard Avenue, observing it to be a one-story ranch house. There were two cars in the driveway: one did not have license plates attached and the other was registered to Kristina Sarin. During the surveillance, Sergeant Faucher noted that there were no unsecure wireless networks.

More than 130 days later, on September 19, 2022, Sergeant Faucher returned to 31 Harvard Avenue, noted the same two cars in the driveway, and again confirmed there were no unsecure wireless networks. Two days after that, on September 21, 2022, Sergeant Faucher filed an application for a search warrant for 31 Harvard Avenue, asserting that Mr. Morin appeared to be using the phone number and the Snapchat account in question and that electronic

devices or digital media in that residence would contain evidence of possession of child pornography.

## ISSUE PRESENTED

1. Whether a delay of more than ten months between reported uploads of child pornography and the application for a search warrant rendered the search warrant stale such that it failed to establish probable cause to search.

This issue was raised in the trial court in a motion to suppress that explicitly raised the issue of staleness. It is thus preserved for this Court's review.

## ARGUMENT

**The delay of more than ten months before seeking a search warrant after reported uploads of child pornography resulted in the search warrant application failing to establish probable cause that the target of the warrant or any electronic devices he controlled would be found in the residence to be searched.**

The delay of more than ten months in seeking a search warrant after reported uploads of child pornography resulted in the warrant application failing to establish probable cause that the target of the warrant, or any electronic devices that he controlled, would be found within the residence to be searched. Because the information in the affidavit was stale, the motion judge erred in denying the motion to suppress.

Under both the United States Constitution and the Massachusetts Declaration of Rights, a search warrant may only issue upon a showing of probable cause. Commonwealth v. Guastucci, 486 Mass. 22, 25 (2020). Probable cause requires that

> the facts contained in an affidavit, plus the reasonable inferences that may be drawn from them, . . . allow the magistrate to determine that the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues."

Id. If the facts set out in the affidavit are too remote, the information can become stale, and the application will fail to establish probable cause. Id. at 26-27.

This Court, among others, has noted that "the determination of staleness in investigations involving child pornography is unique." Id. at 29, quoting United States v. Raymonda, 780 F.3d 105, 114 (2d Cir. 2015). This is so because of the likelihood that individuals who are "interested in" child pornography will "collect and retain such images in the privacy of their own homes." Id. This propensity to retain such images over a long period allows the inference that child pornography is likely to be found on the electronic device of a person "interested in" such images for a longer period. Id. at 30. Thus, information relating to such an investigation is less likely to become stale. See id.

This inference, however, does not mean that applications for search warrants related to child pornography are immune from review for staleness. Id. "Every investigation, including the possession and distribution of child pornography, has a shelf life." Id. In Guastucci, this Court carefully surveyed the jurisprudence in this area, before concluding that the seven-month delay in that case did not render the

information stale. Id. at 27-33. The Court noted, however, that a delay of seven months "may be at the outer limit" of what can survive a staleness challenge. Id. at 27.

This Court's circumspection in the face of reliance on many months' old information was apt. As more time passes, more challenges arise in establishing probable cause that the evidence sought will be located in the place to be searched. See id. at 27, 32 n.4; United States v. Doan, 245 F. App'x 550, 554 (7th Cir. 2007). Although persons "interested in" child pornography may retain images on electronic devices and files may be forensically recovered even "months or years" after being deleted, a search warrant still must establish probable cause that relevant electronic devices or media will be found in the place to be searched. See Guastucci, 486 Mass. at 25, 29. As the delay increases, so does the likelihood that such devices or media will have been discarded due to being damaged, lost, or replaced. See id. at 32 n.4.

In addition, other courts have noted that the relationship between the target and the place to be searched can create a staleness issue. See United States v. Frechette, 583 F.3d 374, 378 (6th Cir. 2009) (noting that whether the target was "nomadic or entrenched" and whether place

to be searched was "mere criminal forum of convenience or secure operational base" relevant to staleness inquiry). Depending on the target's relationship to the place to be searched, a significant delay may decrease the likelihood that a person will still be residing, regularly present, or storing property at that address. See id. For example, an application to search a hotel room or short-term rental for evidence of electronic possession of child pornography would likely be stale where weeks had passed since reported online activity, not because the target was likely to have disposed of any evidence, but because of the low likelihood that electronic devices controlled by the target would still be found in the placed to be searched. Cf. Commonwealth v. Jordan, 469 Mass. 134, 146-147 (2014) (holding no probable cause to search rental car in relation to shooting two days earlier involving rental car in absence of details of rental arrangement).

Notwithstanding reasons for caution in cases of extended delay, the Appeals Court has extended the holding of Guastucci to a search warrant application seeking evidence of child pornography after a delay of eight months. Commonwealth v. Vasquez, Mass. App. Ct., No. 22-P-1134, slip op. at 6 (Nov. 30, 2023). In this case, the delay of ten months

and one week—more than 310 days—extended even further beyond the delay addressed in Guastucci, 486 Mass. at 27. However, neither in this case nor in Vasquez did the court articulate a substantive analysis of how a longer delay affects the probable cause determination. See Guastucci, 486 Mass. at 27; Vasquez, No. 22-P-1134, slip op. at 6.

Properly considered, the effects of the delay in this case were fatal to the probable cause determination. The affidavit identified Mr. Morin as the user of the phone number and Snapchat account that had made the uploads in question. However, the affidavit failed to establish Mr. Morin's current relationship with the residence to searched and thus failed to establish that he or his electronic devices would be found there. The affidavit only set out a limited, historical relationship between Mr. Morin and the residence to be searched. The target residence was a single-story ranch house. The affidavit asserts that there were two listed owners of the residence, neither of whom was Mr. Morin or shared a last name with Mr. Morin. The affidavit did not assert that Mr. Morin was a renter of the property or that he was related to either of the owners. The internet service account was set up in the name of one of the owners of the residence, not Mr. Morin. Surveillance was

made on the house on two separate occasions, but the affidavit does not indicate that officers ever observed Mr. Morin at the residence or observed a vehicle registered to him or associated with him at the residence.

The connection between Mr. Morin and the residence consisted of two items. First, a "registry check of individuals at 31 Harvard Avenue" conducted on May 9, 2022, that "revealed" a driver's license number in Mr. Morin's name. Second, the affidavit recited that a LexisNexis search, inferentially also conducted on May 9, 2022, for the phone number of the phone that was used to upload the reported child pornography "identified an attached individual" as Mr. Morin of 31 Harvard Avenue. The affidavit does not indicate that the "registry check," showed that the license was active at that time, whether there were any other addresses attached to that license, or when the license was last renewed. Nor does the affidavit include any information about whether that cellular phone account remained active, when it was opened, or whether there were any other addresses attached to the account.

Without further information developing Mr. Morin's relationship to the residence, the affidavit failed to establish probable cause that Mr. Morin resided at, regularly accessed, or kept property at the residence at the time of the search in late September of 2022. The information in the affidavit allows the inference that Mr. Morin was present at and used the internet at the residence ten months earlier, in November of 2021. An inference could be drawn that Mr. Morin at one time resided at the residence, such that he used that address to obtain a driver's license and a cellular phone account. However, undated information that he used the address to obtain a driver's license and cellular phone account in combination with Mr. Morin using the internet in the residence ten months prior does not give rise to probable cause that he or his electronic devices would be present in the residence ten months later. In the absence of a showing that Mr. Morin owned, rented, resided, regularly visited, or stored property at the residence at the time of the search, the affidavit fell short of establishing probable cause that Mr. Morin or his electronic devices would be present at the time the warrant was sought. Contrast Guastucci, 486 Mass. at 27.

Addressing a similar issue, a federal court of appeal has noted that "the older the information is regarding child pornography, the more necessary it is to include more detail concerning that information and concerning the person who is the subject of the investigation." United States v. Doan, 245 F. App'x 550, 554 (7th Cir. 2007). Notably, there were numerous ways that investigators in this case could have provided more detail that would have bolstered probable cause that Mr. Morin or his devices would be present in the target residence at the time of the search. Surveillance could have been conducted to establish that Mr. Morin resided at or regularly visited the residence, or that a car Mr. Morin drove was regularly there. An administrative subpoena could have been issued to the internet service provider seeking evidence the phone number or cellular phone related to Mr. Morin were connecting to the internet at the residence close in time to the search warrant application. The affidavit could have included more information about Mr. Morin's driver's license or cellular phone accounts to establish that they were active and that the residence was the most recent or only address listed on the account. The affidavit,

however, lacks any such information that would "freshen" the dated information connecting Mr. Morin to the residence.

In addition, the uploads in this case were made by a cellular phone using a mobile application. Cellular phones, by their nature, are mobile, and most users seldom venture far without their phone. See Riley v. California, 573 U.S. 373, 395 (2014) (noting polling that "three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower"). The improbability that a phone (or its user) would be found at a potential former residence in which the target was last known to be present ten months earlier further illustrates how the passage of time defeated probable cause in this case.

This appeal raises issues not addressed in Guastucci: not only the effect of a delay substantially longer than the seven months addressed in that case, but specifically how the staleness inquiry is affected where the affidavit fails to establish the target as someone who owns, rents, resides, or stores property in the target residence. See Guastucci, 486 Mass. at 27. Due to the limited, dated connections evinced between Mr. Morin and the target residence in this case, the affidavit failed to

establish probable cause to believe that Mr. Morin or electronic devices he controlled would be found there at the time of the search. See Doan, 245 F. App'x at 554.

## REASONS WHY DIRECT APPELLATE REVIEW IS APPROPRIATE

This appeal raises questions concerning the state and federal constitutions "of such public interest that justice requires a final determination by [this] Court." Mass. R.A.P. 11(a). In Guastucci, this court expressed circumspection in holding that a delay of seven months did not render information stale in the context of a child pornography investigation. 486 Mass. at 27. The Appeals Court has extended that holding to a delay of eight months, and the trial court in this case to a delay of more than ten months, both without substantive analysis. As the information relied upon in seeking a search warrant exceeds the seven-month delay in Guastucci, careful analysis is required to ensure that a person's rights to privacy in their homes and electronic devices are only disturbed upon a showing of probable cause. This Court's intervention is necessary to protect those constitutional rights by

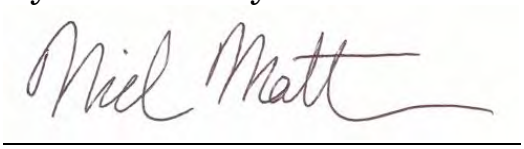
articulating for lower courts the factors to consider in a case where the delay substantially exceeds the delay addressed in Guastucci.

## CONCLUSION

For the reasons explained above, the defendant, Michael Morin, respectfully requests that direct appellate review be allowed.

Respectfully submitted,

MICHAEL MORIN,
By his attorney:



Nicholas Matteson
BBO # 688410
Law Office of Nicholas Matteson
P.O. Box 2633
Holyoke, MA 01041
(857) 415-1608
nm@mattesonlawoffice.com

Dated: April 9, 2026.

## CERTIFICATE OF COMPLIANCE

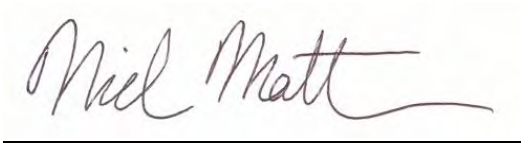
I certify that the foregoing complies with the applicable rules of appellate procedure, including, but not limited to: Rule 11(b) (contents of application for direct appellate review); Rule 20 (form and length of briefs, appendices, and other documents); and Rule 21 (redaction). Compliance with Mass. R.A.P. 11(b) was ascertained using the word count feature of Microsoft Word for Mac, version 16.107.3. This Application for Direct Appellate Review has been produced using 14-point Century Schoolbook, a proportionally spaced font. The number of words in the argument section of the Application is 1,911.

Nicholas Matteson

## CERTIFICATE OF SERVICE

I hereby certify, under pains and penalties of perjury, that I have on this date made service upon the Commonwealth by directing a copy of this application for direct appellate review be electronically served by the Court's e-file protocol on the following counsel for the Commonwealth:

Assistant District Attorney Ellyn H. Lazar
Worcester County District Attorney's Office
225 Main Street, Room G301
Worcester, MA 01608
508-755-8601



Nicholas Matteson
BBO # 688410
Law Office of Nicholas Matteson
P.O. Box 2633
Holyoke, MA 01041
(857) 415-1608
nm@mattesonlawoffice.com

Dated: April 9, 2026

# CRIMINAL DOCKET

| DOCKET NUMBER | NO. OF COUNTS | Trial Court of Massachusetts District Court Department |
|---|---|---|
| 2367CR001631 | 1 | |

| DEFENDANT NAME AND ADDRESS | DOB | GENDER | COURT NAME & ADDRESS |
|---|---|---|---|
| Michael S Morin<br>31 Harvard Avenue<br>Shrewsbury, MA 01545 | 12/22/1988 | Male | Westborough District Court<br>186 Oak Street<br>Westborough, MA 01581 |
| | DATE COMPLAINT ISSUED<br>11/30/2023 | | |
| | PRECOMPLAINT ARREST DATE | | INTERPRETER REQUIRED |

FIRST FIVE OFFENSE COUNTS

| COUNT | CODE | OFFENSE DESCRIPTION | OFFENSE DATE |
|---|---|---|---|
| 1 | 272/29C/A | CHILD PORNOGRAPHY, POSSESS c272 §29C | 09/21/2022 |

Courtney Sans
ADA Katie Becker

Nicholas Matteson 12/30/25

| DEFENSE ATTORNEY | OFFENSE CITY/TOWN | POLICE DEPARTMENT |
|---|---|---|
| DANIEL CAPPETTA | Shrewsbury | Shrewsbury PD |

| DATE & JUDGE | DOCKET ENTRY | DATE & JUDGE | FEES IMPOSED |
|---|---|---|---|
| 12/11/23 Longton NO. Plea | ☐ Attorney appointed (SJC R. 3:10)<br>☐ Atty denied & Deft. Advised per 211 D §2A<br>☐ Waiver of Counsel found after colloquy<br>BDP cont | | Counsel Fee (211D § 2A¶2) $ ☐ WAIVED<br>Counsel Contribution (211D § 2) $ ☐ WAIVED |
| | **Terms of release set:** ☐ PR ☐ Bail<br>☑ See Docket for special condition<br>☐ Held (276 §58A) | | Default Warrant Fee (276 § 30¶1) $ ☐ WAIVED<br>Default Warrant Arrest Fee (276 § 30 ¶2) $ ☐ WAIVED |
| 12/11/23 Longton | **Arraigned and advised:**<br>☑ Potential of bail revocation (276 §58B)<br>☐ Right to bail to review (276 §58)<br>☐ Right to drug exam (111E § 10)<br>☐ Inquiry made by Court under 276 § 56A | | Probation Supervision Fee (276 § 87A) $ ☐ WAIVED<br>Bail Order Forfeited<br>**Advised of right to jury trial:**<br>☐ Waiver of jury found after colloquy<br>☐ Does not waive |
| | **Abuse Allegation:**<br>☐ C276 § 56A form filed by Commonwealth<br>☐ Allegation of abuse under C276 § 56A found<br>☐ No allegation of abuse under C276 § 56A found | | Advised of trial rights as pro se (Dist. Ct. Supp.R.4)<br>Advised of right of appeal to Appeals Ct. (M.R. Crim P.R. 28) |

**SCHEDULING HISTORY**

| NO. | SCHEDULED DATE | EVENT | RESULT | JUDGE | TAPE START/ STOP |
|---|---|---|---|---|---|
| 1 | 12/11/2023 | Arraignment | ☑ Held ☐ Not Held but Event Resolved ☐ Cont'd | Longton | |
| 2 | 2/14/24 | PTH | ☐ Held ☐ Not Held but Event Resolved ☑ Cont'd | Callahan | |
| 3 | 4.22.24 | PTH | ☑ Held ☐ Not Held but Event Resolved ☐ Cont'd | Callahan | |
| 4 | 6.4.24 | DCE | ☐ Held ☐ Not Held but Event Resolved ☑ Cont'd | Stark | |
| 5 | 6.14.24 | DCE | ☐ Held ☐ Not Held but Event Resolved ☑ Cont'd | STARK | |
| 6 | 8/23/24 | C+R | ☑ Held ☐ Not Held but Event Resolved ☐ Cont'd | Despotopoulos | |
| 7 | 11.12.24 | PRD | ☐ Held ☐ Not Held but Event Resolved ☑ Cont'd BF | Stark | |
| 8 | 12.9.24 | PRD | ☐ Held ☐ Not Held but Event Resolved ☐ Cont'd | | |
| 9 | 1-23-25 | PRD | ☐ Held BF ☐ Not Held but Event Resolved ☐ Cont'd | | |
| 10 | 3-14-25 | PRD | ☐ Held ☑ Not Held but Event Resolved ☐ Cont'd | Stark | |

**APPROVED ABBREVIATIONS**

ARR = Arraignment PTH = Pretrial hearing DCE = Discovery compliance & jury selection BTR = Bench trial JTR = Jury trial PCH = Probable cause hearing MOT = Motion hearing SRE = Status review SRP = Status review of payments FAT = First appearance in jury session SEN = Sentencing CWF = Continuance-without-finding scheduled to terminate PRO = Probation scheduled to terminate DFTA = Defendant failed to appear & was defaulted WAR = Warrant issued WARD = Default warrant issued WR = Warrant or default warrant recalled PVH = probation revocation hearing.

| A TRUE COPY ATTEST: | CLERK-MAGISTRATE / ASST CLERK | TOTAL NO. OF PAGES | ON (DATE) |
|---|---|---|---|
| | X | | |

Date/Time Printed: 11-30-2023 09:51:51

2367CR001631

Revised: 07/16

5/13/25 (M). Non evidentiary

BF STARK

# CRIMINAL DOCKET - OFFENSES

DEFENDANT NAME: Michael S Morin

DOCKET NUMBER: 2367CR001631

COUNT / OFFENSE: 1 CHILD PORNOGRAPHY, POSSESS c272 §29C

DISPOSITION DATE AND JUDGE: 12/11/25 Eustis

DISPOSITION METHOD

☑ Guilty Plea or ☐ Admission to Sufficient Facts accepted after colloquy and alien warning pursuant to C278§29D and MRCrP12

☐ Bench Trial

☐ Jury Trial

☐ Dismissed upon:

☐ Request of Commonwealth ☐ Request of Victim

☐ Request of Defendant ☐ Failure to prosecute

☐ Other:

☐ Filed with Defendant's consent — submit treatment plan + Eval to prob.

☐ Nolle Prosequi

☐ Decriminalized (277 §70 C) — Sign releases to Prob

| FINE/ASSESSMENT | SURFINE | COSTS | OUI §24D FEE | OUI VICTIMS ASMT |
|---|---|---|---|---|
| | | | | |
| **HEAD INJURY ASMT** | **RESTITUTION** | **V/W ASSESSMENT** | **BATTERER'S FEE** | **OTHER** |
| | | | | |

SENTENCE OR OTHER DISPOSITION

☐ Sufficient facts found but continued without a finding until:

☑ Defendant placed on probation until: 2 year 12/7/27

☑ Risk/Need or OUI ☐ Administrative Supervision

☐ Defendant placed on pretrial probation (276 §87) until:

☐ To be dismissed if court costs / restitution paid by: forfeit devices to law enforcement

# 9, 13, 16 Conditions by Prob.

New MH Eval, Continue w/ treatment currently in.

No unsupervised contact w/ children under 16

FINDING

☑ Guilty ☐ Not Guilty

☐ Responsible ☐ Not Responsible

☐ Probable Cause ☐ No Probable Cause

FINAL DISPOSITION JUDGE DATE

☐ Dismissed on recommendation of Probation Dept.

☐ Probation terminated: defendant discharged

☐ Sentence or disposition revoked (see cont'd page)

---

COUNT / OFFENSE

DISPOSITION DATE AND JUDGE

DISPOSITION METHOD

☐ Guilty Plea or ☐ Admission to Sufficient Facts accepted after colloquy and alien warning pursuant to C278§29D and MRCrP12

☐ Bench Trial

☐ Jury Trial

☐ Dismissed upon:

☐ Request of Commonwealth ☐ Request of Victim

☐ Request of Defendant ☐ Failure to prosecute

☐ Other:

☐ Filed with Defendant's consent

☐ Nolle Prosequi

☐ Decriminalized (277 §70 C)

| FINE/ASSESSMENT | SURFINE | COSTS | OUI §24D FEE | OUI VICTIMS ASMT |
|---|---|---|---|---|
| | | | | |
| **HEAD INJURY ASMT** | **RESTITUTION** | **V/W ASSESSMENT** | **BATTERER'S FEE** | **OTHER** |
| | | | | |

SENTENCE OR OTHER DISPOSITION

☐ Sufficient facts found but continued without a finding until:

☐ Defendant placed on probation until:

☐ Risk/Need or OUI ☐ Administrative Supervision

☐ Defendant placed on pretrial probation (276 §87) until:

☐ To be dismissed if court costs / restitution paid by:

FINDING

☐ Guilty ☐ Not Guilty

☐ Responsible ☐ Not Responsible

☐ Probable Cause ☐ No Probable Cause

FINAL DISPOSITION JUDGE DATE

☐ Dismissed on recommendation of Probation Dept.

☐ Probation terminated: defendant discharged

☐ Sentence or disposition revoked (see cont'd page)

---

COUNT / OFFENSE

DISPOSITION DATE AND JUDGE

DISPOSITION METHOD

☐ Guilty Plea or ☐ Admission to Sufficient Facts accepted after colloquy and alien warning pursuant to C278§29D and MRCrP12

☐ Bench Trial

☐ Jury Trial

☐ Dismissed upon:

☐ Request of Commonwealth ☐ Request of Victim

☐ Request of Defendant ☐ Failure to prosecute

Other:

☐ Filed with Defendant's consent

☐ Nolle Prosequi

☐ Decriminalized (277 §70 C)

| FINE/ASSESSMENT | SURFINE | COSTS | OUI §24D FEE | OUI VICTIMS ASMT |
|---|---|---|---|---|
| | | | | |
| **HEAD INJURY ASMT** | **RESTITUTION** | **V/W ASSESSMENT** | **BATTERER'S FEE** | **OTHER** |
| | | | | |

SENTENCE OR OTHER DISPOSITION

☐ Sufficient facts found but continued without a finding until:

☐ Defendant placed on probation until:

☐ Risk/Need or OUI ☐ Administrative Supervision

☐ Defendant placed on pretrial probation (276 §87) until:

☐ To be dismissed if court costs / restitution paid by:

FINDING

☐ Guilty ☐ Not Guilty

☐ Responsible ☐ Not Responsible

☐ Probable Cause ☐ No Probable Cause

FINAL DISPOSITION JUDGE DATE

☐ Dismissed on recommendation of Probation Dept.

☐ Probation terminated: defendant discharged

☐ Sentence or disposition revoked (see cont'd page)

| CRIMINAL DOCKET<br>DOCKET ENTRIES | DEFENDANT NAME<br>Michael S Morin | DOCKET NUMBER<br>2367CR001631 |
|---|---|---|

| DATE | DOCKET ENTRIES |
|---|---|
| 11.30.2023 | SUMMONS Mailed |
| 12-6-23 | Appearance filed by Atty Cappetta |
| 12.11.23 | Conditions of Release - No unsupervised contact w/ Children under 16 - NO out of State travel. Longston, J |
| 6/27/24 | Defendant's ex-parte motion for funds to evaluate the Defendant's risk of future offenses is allowed Stark |
| 4/1/25 | D's Motion to Suppress filed. |
| 5/12/25 | Def. attny filed mot. to continue - allowed + Cont. to 6/13/25 MOT - Stark |
| 6-13-25 | MTS held - @ 10:25AM Ctroom 2. |
| | Taken under - Hon. N. Longston. C to |
| | 8.4.25 @ 9AM - Status. N. Longston |
| 8.4.25 | Motion still under advisement C-9-19-25 for SRE |
| 8-12-25 | Motion to suppress Denied by Judge Longston. |
| | Both Parties Notified |
| 9/19/25 | D's (M) for funds filed + allowed. (J. Greenhalgh) |
| 11/7/25 | Dispo. |
| 9/25/25 | Atty Cappetta files motion to change date, motion is heard and Allowed, Greenhalgh J |
| | C-12/11/25 for pres. |
| 12/11/25 | After full dispo, Dft counsel requests Sorb Hearing under 178A - After full hearing re: Sorb registration, Dft will not have to register after Judges ruling Curtis J |

**APPROVED ABBREVIATIONS**
ARR = Arraignment PTH = Pretrial hearing DCE = Discovery compliance & jury selection BTR = Bench trial JTR = Jury trial PCH = Probable cause hearing MOT = Motion hearing SRE = Status review
SRP = Status review of payments FAT = First appearance in jury session SEN = Sentencing CWF = Continuance-without-finding scheduled to terminate PRO = Probation scheduled to terminate
DFTA = Defendant failed to appear & was defaulted WAR = Warrant issued WARD = Default warrant issued WR = Warrant or default warrant recalled PVH = probation revocation hearing

| CRIMINAL DOCKET DOCKET ENTRIES | DEFENDANT NAME Michael S Morin | DOCKET NUMBER 2367CR001631 |
|---|---|---|

| DATE | DOCKET ENTRIES |
|---|---|
| | 12-11-25 Joint Statement Re: Tender of Plea Pursuant to M.R.C.P. 12(b)(6). |
| 12/18/25 | Notice of appeal of ruling on motion to suppress filed. |
| 1-13-26 | Motion to revise + revoke sentence filed |
| 1-29-26 | Transcript ordered for Appeal on Motion to revise + revoke |
| 3/2/26 | Transcript received via email from Transcription Services Parties notified of Assembly of Record. |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

APPROVED ABBERIVATIONS
ARR = Arraignment PT= Pretrial hearing CE = Discovery compliance & jury selection T = Bench trial JT = Jury trial PC = Probable cause hearing M = Motion hearing SR= Status review
SRP = Status review of payments FA = First appearance in jury session S = Sentencing CW = Continuance-without-finding scheduled to terminate P = Probation scheduled to terminate
DFTA = Defendant failed to appear & was defaulted WAR = Warrant issued WARD = Default warrant issued WR = Warrant or default warrant recalled PR = probation revocation hearing

DENIED. The search warrant was based on probable cause. Though there was a delay between the initial investigation and application for a search warrant, the Court does not find it to be unconstitutional. Guastucci, 484 Mass. 237 (2020) does not hold otherwise.

Lynch, J.
8/12/25

**COMMONWEALTH OF MASSACHUSETTS**

**WORCESTER COUNTY** **WESTBOROUGH DISTRICT COURT**
**DOCKET 2367CR001631**

**COMMONWEALTH**

**V.**

**MICHAEL MORIN**

**DEFENDANT'S MOTION TO SUPPRESS EVIDENCE**

Now comes, Michael Morin, the defendant in the above-captioned case, and respectfully moves this honorable court to suppress all evidence recovered during a search of Mr. Morin's apartment executed by members of the Shrewsbury Police Department pursuant to a search warrant on September 21, 2022. Such evidence includes, but is not limited to, any and all evidence seized during the search of Mr. Morin's home on the above referenced date.

As grounds therefore, Mr. Morin states the search warrant authorizing the search was issued without probable cause. Mr. Morin further states that the search warrant violated the particularity requirements of the state and federal constitutions. As such, the search pursuant to the warrant violated Mr. Morin's rights under article 14 of the Massachusetts Declaration of Rights and the Fourth and Fourteenth Amendments to the United States Constitution.

Respectfully submitted,
MICHAEL MORIN,
By his attorney:

Daniel Cappetta, BBO # 665860
Cappetta Law Offices
150 Speen St, Suite 201
Framingham, MA 01701
(508) 762-4540

Dated: March 31, 2025

TYPED VERSION OF HANDWRITTEN ENDORSEMENT ON MOTION TO SUPPRESS

DENIED. The search warrant was based on probable cause. Though there was a delay between the initial investigation and application for a search warrant, the Court does not find it to be unconstitutional. Guastucci, 486 Mass. 22, 27 (2020) does not hold otherwise.

Longton, J.
8/12/25

# APPLICATION FOR SEARCH WARRANT
G.L. c. 276, §§ 1-7

TRIAL COURT OF MASSACHUSETTS

District COURT DEPARTMENT

Westborough DIVISION

NAME OF APPLICANT
David J. Faucher

POSITION OF APPLICANT
Sergeant

SEARCH WARRANT DOCKET NUMBER
225W0068

I, the undersigned **APPLICANT**, being duly sworn, depose and say that:

1. I have the following information based upon the attached affidavit(s), consisting of a total of 27 pages, which is (are) incorporated herein by reference.
2. Bases upon this information, there is **PROBABLE CAUSE** to believe that the property described below:

- ☐ has been stolen, embezzled, or obtained by false pretenses.
- ☑ is intended for use or has been used as the means of committing a crime.
- ☑ has been concealed to prevent a crime from being discovered.
- ☑ is unlawfully possessed or concealed for an unlawful purpose.
- ☑ is evidence of a crime or is evidence of criminal activity.
- ☐ other *(specify)* _____

3. I am seeking the issuance of a warrant to search for the following property *(describe the property to be searched for as particularly as possible):*

The property list is too extensive. Please refer to "Appendix A" for the detailed list of property that the applicant is seeking.

4. Based upon this information, there is also probable cause to believe that the property may be found *(check as may as apply):*

☑ at *(identify the exact location or description of the place(s) to be searched):*

31 Harvard Avenue Shrewsbury Massachusetts 01545. The residence is a white single story ranch with a driveway on the left side. The number "31" is clearly visible on the house between the garage and a red entry door.

which is occupied by and/or in possession of:

Linda Carpenter DOB 10/02/1942 MA License [redacted]5116 Michael Morin DOB 12/22/1988 MA License [redacted]7028
Kristina Sann MA License [redacted]1778 DOB 9/03/1987

☑ on the person or in the possession of *(identify any specific person(s) to be searched):*

Michael Morin DOB 12/22/1988 MA License [redacted]7028

☑ on any person present who may be found to have such property in his or her possession or under his or her control or to whom such property may have been delivered.

THEREFORE, I respectfully request that the court issue a Warrant and order of seizure, authorizing the search of the above described place(s) and person(s), if any, to be searched, and directing that such property or evidence or any part thereof, if found, be seized and brought before the court, together with such other and further relief that the court may deem proper.

- ☐ have previously submitted the same application.
- ☑ Have not previously submitted the same application.

PRINTED NAME OF APPLICANT
David J. Faucher

SIGNED UNDER THE PENALTIES OF PERJURY
X _____
Signature of Applicant

SWORN AND SUBSCRIBED TO BEFORE
X _____
Signature of Justice, Clerk-Magistrate or Assistant Clerk

9/21/2022
DATE

## AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

1. I, **Sergeant David Faucher**, being duly sworn, depose and say:

2. I, David J. Faucher, am assigned as a uniformed Sergeant of the Patrol Division for the Town of Shrewsbury Police Department. I hold a Bachelor's Degree of Science from Westfield State College and a Master's Degree in Criminal Justice from Anna Maria College. I have been employed as an officer in the Town of Shrewsbury since December 10, 2007. I attended the MBTA Transit Police Academy in Quincy, Massachusetts where I received instruction in criminal investigations as well as criminal and constitutional law. During my time as an officer with the department, I have been involved in a variety of criminal cases as well as hundreds of arrests. As a patrolman, a Detective and now a Sergeant, I have had the opportunity to lead and assist on a variety of cases including internet crimes, narcotics investigations, larcenies, identity theft, breaking and entering, and the apprehension of criminals for various criminal acts.
   Throughout my career, I have had the opportunity to participate in various training courses on the search and seizure of property. I have attended the DEA Basic Narcotics Investigator School and have been certified as a Sexual Assault Investigator. As a member of the Internet Crimes Against Children Task Force (ICAC), I have been part of numerous investigations that have led to various types of searches and seizures of residences and personal property of suspects. I have conducted and assisted with various search warrants that have led to the arrest and conviction of the suspects.

3. This affidavit has attached hereto and incorporated herein by reference the following attachments:

   a. Exhibit 1: An **eleven (11) page** document providing background information on computer systems.
   b. Exhibit 2: A **one (1) page** image of residence at **31 Harvard Avenue, Shrewsbury MA 01545**.

   c. Appendix A: A **five (5) page** document detailing the items to be searched for at the search location, **31 Harvard Avenue, Shrewsbury MA 01545.**

4. The facts establishing the grounds for my request to the court for the issuance of a search warrant are as follows:

5. On February 22, 2022, I received a CyberTip report from Trooper Christopher Macdonald of the Massachusetts State Police. The report, numbered #107031090, was received by the National Center for Missing and Exploited Children on November 14, 2021. The report was then made available to Lieutenant Katrina Mazzie of the Massachusetts State Police on December 21,

2021. This report had been generated by the National Center for Missing and Exploited Children in reference to a submission by electronic service provider, Snapchat, Records Custodian 2772 Donald Douglas Loop N, Santa Monica, California 90405.

6. The National Center for Missing and Exploited Children® (NCMEC) was established in 1984 as a private, nonprofit 501(c) (3) organization. NCMEC provides services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. I am also aware from my experience working on child sexual exploitation investigations that NCMEC launched the CyberTipline on March 9, 1998, to serve as the national clearinghouse for tips and leads about child sexual exploitation. The CyberTipline (www.missingkids.org/cybertipline) was developed to further NCMEC's mission of helping prevent and diminish the sexual exploitation of children by allowing the public and electronic service providers ("ESP's") to report online (and via toll-free phone) the enticement of children for sexual acts, extra-familial child sexual molestation, child pornography, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, misleading words, or digital images on the Internet. A secure CyberTipline was created in February 2000 to facilitate the reporting of apparent child pornography by ESP's. Once registered with NCMEC, ESP's can upload files relating to child sexual exploitation content when making reports to NCMEC using a secure electronic connection. Uploaded image files may include images, video or other reported content. Neither the government nor any law enforcement agency created the CyberTipline or has input into CyberTipline operations. The government does not instigate, direct, or provide guidance to NCMEC in its processing of CyberTipline reports. NCMEC staff cannot alter or change information submitted by a reporting ESP. NCMEC does not direct or mandate the type of information that an ESP may choose to submit in a CyberTipline report, but instead provides voluntary reporting fields that ESP's may populate with information, including uploading apparent child pornography image files. After an ESP makes a CyberTipline report to NCMEC, a staff member uses conventional and publicly-available open source tools to try to identify potential geographic information pertaining to the individual who is the subject of the report as well as geographic information of the ESP potentially used in connection with the reported image files. NCMEC is required only to make CyberTipline reports available to law enforcement. NCMEC is not required to open reported image files or review any content provided by a member of the public or an ESP in a CyberTipline report. If NCMEC independently decides to open a reported image file or review the contents of a CyberTipline report, it does so pursuant to its internal organizational and operational guidelines and in furtherance of its private mission to aid children. NCMEC does not open or view every image file submitted in a CyberTipline report. Pursuant to NCMEC's current review process, NCMEC staff make an independent determination whether to open reported image files based on operational factors, including but not limited to the volume of reports, whether a child might be in imminent danger, and the need to determine a potential geographic location of a child or reported user. After an



C. J.

Exploited Child Division staff member at NCMEC has determined a potential geographical location and completed processing the CyberTipline report, the report is made available to a law enforcement agency in the potential geographic location for independent review and potential investigation. CyberTipline reports are made available to law enforcement in this way through the use of a secure virtual private network owned and operated by NCMEC

7. Snapchat is a mobile application made by Snap Inc. ("Snap") and available through the iPhone App Store and Google Play Store. The Snapchat app provides users a way to share moments with photos, videos, and chats.

8. Snapchat identified 9 files that had been disseminated on November 13, 2021 and identified the User who uploaded the files as:

   Screen/User Name: mikle888
   Phone: 774-253-5696
   Date of Birth: 12-22-1988
   IP address: 2600:1000:b0d:26ea:7416:ac90:5572:5306

9. I have personally viewed the files as a result of the CyberTip and identified them as child pornography, also known as child sexual abuse material (CSAM). Based upon my training and experience, each of the digital files appears to be Child Pornography in violation of Massachusetts General Law Chapter 272 §§ 29 (governing obscene matter crimes), 29B (governing the crime of the possession with intent to disseminate child pornography), and 29C (governing the crime of the possession of child pornography).

10. Contained within the CyberTip were the original file names along with the MD5 Hash values of the images supplied. The uploaded files identified within the Cybertip are as follows:

    Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~417-4c7eda5c4a.jpg
    MD5: 3de3d44692a389668f0afce9475ab8a5
    Additional Information: 2021-11-13T10:26:25Z this timestamp is when the user sent this media file
    *The image uploaded depicts a young prepubescent white female facing away from the camera in a position where she is bent over at the waist with her clothing pulled down exposing her vagina and buttocks.*

    Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~391-93dd7d7cd1.jpg
    MD5: 93de5add6eaf864088dfb1827ffc1998
    Additional Information: 2021-11-13T10:20:18Z this timestamp is when the user sent this media file
    *The image uploaded depicts a prepubescent female estimated to be approximately*



C. J.

*four to six years old. The female is unclothed laying on a bed with her legs spread. An adult male penis is penetrating the female's vagina and the female appears to be crying and in distress.*

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~386-cef3c00735.jpg
MD5: 15c129ea18afee22b2edd30bf5cb3e1d
Additional Information: 2021-11-13T10:18:00Z this timestamp is when the user sent this media file
*The image uploaded depicts a prepubescent female unclothed on the backseat of what appears to be a vehicle. The female, whose face is out of view, is facing towards the camera with what appears to be an adult male holding the female under her arms while penetrating the female's vagina with his penis.*

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~424-3af52078f9.jpg
MD5: b0166c8fda6eb6620b55e63cb89186f0
Additional Information: 2021-11-13T10:29:49Z this timestamp is when the user sent this media file
*The image uploaded depicts a prepubescent white female who has no pants or underwear on. The female his holding her leg in the air exposing her vagina.*

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~422-a351862280.jpg
MD5: ca362cd2229d5dd0f3a0f265fd4755e9
Additional Information: 2021-11-13T10:28:37Z this timestamp is when the user sent this media file
*The image uploaded depicts a prepubescent male completely unclothed. The male's penis is erect and it appears he is holding what appears to be a cigarette in his hand.*

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~447-0febc3eac6.jpg
MD5: 2f4f485d00f12d5eb4d642d66347494f
Additional Information: 2021-11-13T10:38:38Z this timestamp is when the user sent this media file
*The image uploaded depicts a prepubescent white female who is completely unclothed. The female is holding what appears to be the erect penis of a white male in her hand while she is positioned with her legs spread and her vagina exposed.*

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~443-1d15d00e88.jpg
MD5: 63db5d40e4484f87e01179c1c6c3d20f
Additional Information: 2021-11-13T10:35:16Z this timestamp is when the user sent this media file
*The image uploaded depicts a white prepubescent male and a white prepubescent*



C. J.

*female on a white couch. The male is completely unclothed with his leg on top of the female's leg who is laying opposite him. The female is unclothed and is positioned in a way that her leg is under the male's and her other leg is bent towards her exposing her vagina.*

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~331-1fd3f85c3b.jpg
MD5: 298528873888841195fa2e8ad9137781
Additional Information: 2021-11-13T09:15:53Z this timestamp is when the user sent this media file
*The image uploaded depicts a prepubescent white female completely unclothed standing in front of trees exposing both her breast and vagina.*

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~157-500747a6f3.jpg
MD5: 8f6d98a7517ac3cb8deab8333c104516
Additional Information: 2021-11-13T01:59:26Z this timestamp is when the user sent this media
*The uploaded image depicts a prepubescent female and an adult female in a shower setting. The prepubescent female is standing in front of the adult female with her front positioned towards the camera exposing her chest and vagina.*

11. I understand MD5 hashing to be a form of cryptography whose main purpose is to verify that a file has been unaltered. Cryptography in general, is the practice which involves the creation of codes that allows information to be kept secret and unreadable to an unauthorized user. MD5 confirms that two sets of data are identical by comparing raw data by producing and comparing checksums. A checksum is a sequence of numbers and letters used to check data for errors. The hash value assigned to a file is unique to that file's contents, and that file only. Like a fingerprint for the file, if the contents of the file are changed, the hash value will also change.

12. As shown above, Snapchat identified the IP address of the user uploading all of the files identified as child pornography as: **2600:1000:b0d:26ea:7416:ac90:5572:5306**

13. An IP address is a unique string of numbers all information technology devices (computers, printers, modems, etc...) use which identifies and allows them the ability to communicate with each other on a computer network. In layman's terms it is the same as your home address. In order for you to receive postal mail at home, the sending party must have your correct mailing address (IP address) in your town (network). The same is true for all equipment on the internet. Without this specific address, information cannot be received.

14. On December 23, 2021, an administrative subpoena for the IP address **2600:1000:b0d:26ea:7416:ac90:5572:5306,** was issued and sent to Verizon. As a result of the Administrative Subpoena, the electronic service provider, Verizon,

provided the following records and other information pertaining to its respective subscriber:

**Name:** Linda Carpenter
**Address** 31 Harvard Avenue Shrewsbury MA 01545
**Account:** 786126689-1
**Phone:** 774-253-5696
**IMEI:** 359551080450777
**MFG_NAME:** Motorola
**EQP_NAME:** Moto Z2 Force Gold

15. On May 9, 2022 I ran a registry check of individuals at 31 Harvard Avenue. My investigation revealed:
    a. Linda Carpenter MA License [redacted]5116 DOB 10/02/1942
    b. Michael Morin MA License [redacted]7028 DOB 12/22/1988, and a certain social security number
    c. Kristina Sarin MA License [redacted]1778 DOB 9/03/1987

16. A check of the Shrewsbury GIS online directory showed the residence to be owned by Sajiv Sarin with a co-owner being identified as Linda Carpenter since 6/01/1995.

17. A check of Lexis Nexis of the phone number 774-253-5696 identified an attached individual as Michael Morin of 31 Harvard Avenue, Shrewsbury MA 01545, with the same social security number found in the registry records cited above.

18. Based on the information received in the Cybertip from Snapchat, and the investigation into the residents at 31 Harvard Avenue, it does appear that Michael Morin uses the phone number 774-253-5696 and is utilizing the screen name "mikle888" as the birthday provided from Snapchat matches Michael's date of birth of 12/22/1988.

19. On May 11, 2022, at approximately 1116 hours, I went to 31 Harvard Avenue, Shrewsbury MA. I observed the residence to be a white ranch-style home with a driveway on the left side of the property leading to a garage door. I observed two vehicles in the driveway:
    a. A gold Kia Soul with no plates on it
    b. MA registration 93BX02 a 2011 Cadillac registered to Kristina Forslund Sarin.

20. On May 11, 2022, while conducting physical surveillance of the residence I detected that all wireless networks were secure.

21. On September 19, 2022 I returned to the residence and observed the Kia Soul in the driveway. The black Cadillac was also present. A scan of the wireless networks in front of the residence again yielded no unsecure networks.

22. The residence at 31 Harvard Avenue, Shrewsbury MA, is a white, one-story ranch style home. Entrance to the property is through the driveway on the left side of the property. There is an attached garage situated on the left side of the property. The number "31" is clearly displayed to the right of the garage in between the garage door and a red entry door that faces the road. There appears to be another red entry door towards the center of the residence that faces north. There is one electric meter visible from the street on the garage side of the residence.

23. I know from training and experience that those who have possessed and/or disseminated child pornography have an interest or preference in the sexual activity of children. Those who have demonstrated an interest or preference in sexual activity with children or in sexually explicit visual images depicting children are likely to keep secreted, but readily at hand, sexually explicit visual images depicting children. In some instances, these depictions are actual photographs or images of the suspect's own sexual activity with past or present children. In some instances, the suspect keeps these depictions as a means of plying, broaching, or titillating the sexual interests of new child victims or otherwise lowering the inhibitions of other potential child sexual partners by showing them that other children participate in this kind of activity. Still, in other instances, the depictions are a means of arousing the suspect. These depictions tend to be extremely important to such individuals and are likely to remain in the possession of or under the control of such an individual for extensive time periods. A person who has this type of material is not likely to destroy the collection. These sexually explicit visual images depicting children can be in the form of, but not limited to, negatives, slides, books, magazines, videotapes, photographs or other similar visual reproduction, or by an image/video depiction by computer.

24. I know from training and experience that persons trading in, receiving, distributing, or possessing images or movies involving child pornography will often make copies of those files on their computer's hard drive or other removable media. These computer storage media devices can be and have been found within the person's residence, on the person, and within their motor vehicles.

25. I know from my training and experience that even if files were deleted by a user, they still may be recoverable by a trained computer forensic examiner. Please refer to paragraph Z of Exhibit 1 for a discourse about the likelihood of a deleted file being discovered months or years after it has been deleted.

26. I know from training and experience that persons trading in, receiving, distributing, or possessing images or movies involving the exploitation of children, or those interested in the actual exploitation of children, often communicate with others



C.J.

through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a person's interest in child pornography or child exploitation.

27. I know from training and experience that individuals who have a sexual interest in children and have access to the Internet will often conduct searches for child pornography and child sex stories on the Internet using Internet search engines or other programs that share files via the Internet. These individuals will use terms that are associated with children, nudity, and sex. These searches can be found within Internet history files, such as Internet Explorer History, or within unallocated areas of the hard drive.

28. I know from training and experience that files related to the exploitation of children found on computers are usually obtained from the Internet using application software which often leaves files, logs, or file remnants, which would tend to show the exchange, transfer, distribution, possession, or origin of the files.

29. I know from training and experience that computers used to access the Internet usually contain files, logs, or file remnants, which would tend to show ownership and use of the computer as well as ownership and use of Internet service accounts used for the Internet access.

30. I know from training and experience that search warrants for residences involved in computer-related criminal activity usually produce items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence, and other identification documents.

31. I know from training and experience that search warrants for residences usually reveal items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements, and other identification documents.

32. I also have the knowledge, based upon my experience and training, that if untrained persons are allowed into a crime scene, they may unintentionally disturb, damage, or obliterate crucial evidence. Accordingly, while the crime scene search warrant is being executed, I respectfully seek the court's authority to impound and secure the premises and to keep out all unauthorized persons not assigned to the investigation.

33. Based upon your affiant's training and experience, and the collective knowledge of the other officers that your affiant has worked with on this investigation, your affiant asserts that there is probable cause to believe that computer(s) and/or digital media located inside the residence at **31 Harvard Avenue, Shrewsbury MA**, have possessed and disseminated child sexual abuse material (CSAM). This digital media, or computer(s), have been used to facilitate possession of obscene material, a violation of Massachusetts General Law, Chapter 272, Section 29; possession of

visual material of a child depicted in sexual conduct, a violation of Massachusetts General Law, Chapter 272, Section 29C; and dissemination of visual material of a child in a state of nudity, a violation of Massachusetts General Law, Chapter 272, Section 29B/A; and will be located at the residence located at 31 Harvard Avenue, Shrewsbury, MA 01545.

34. I respectfully request that the Court issue a warrant and order of seizure, authorizing the search of the property located at **31 Harvard Avenue, Shrewsbury MA 01545, located in Shrewsbury, Massachusetts** described previously in above Paragraph **#22**, and search for those items listed in "Appendix A" (and with regard to such "computer systems" to transport the same to a secure location anywhere in the Commonwealth of Massachusetts and, there, to SEARCH therein for and SEIZE the items listed in Appendix A). Said "Appendix A" will be attached to the face of the warrant.

35. Your affiant also seeks authorization to copy digital evidence stored on a server (or servers) in another location if a server can be remotely accessed from a computer (or computers), a tablet (or tablets), and/or a cell phone (or cell phones) located at the site authorized to be searched by this warrant. This authorization would permit law enforcement to preserve the integrity of such evidence and prevent it from being tampered with or destroyed. Your affiant knows, through my training and experience, that so-called "cloud service providers" are quite common. Such providers store data on remote servers that customers can access from their home or any other location with Internet access. Examples of these services include Dropbox, Google Drive, Picasa, Apple's iCloud, Microsoft SkyDrive, and Microsoft's OneDrive. These services also encompass common "web mail" such as Hotmail, Gmail and Yahoo! mail. Customers can view, alter, create, copy and print data from these remote servers as if it was at the same location as the customer. The customer typically owns and controls the data stored at the remote server while the electronic service provider owns the server on which the data is stored. In your affiant's training and experience, law enforcement commonly do not discover that a target of a search warrant is utilizing a cloud service provider until the service of a search warrant takes place. Preservation of "cloud data" accessible by computers targeted by this warrant is paramount. After a connection to a cloud computing service is discovered, it could take law enforcement hours or days to obtain a second search warrant targeted at the service provider operating that service. But it could take mere seconds for data to be deleted from that service remotely from anywhere in the world with an Internet connection. Furthermore, should a connection with a cloud computing service be closed as a result of the powering down and seizing of a computer authorized to be seized by this warrant, encryption mechanisms could prevent such a connection from being reopened and the data accessed in the future. Depending on the cloud service provider, should an open connection to the provider be closed, such encryption may not even be able to be bypassed should a warrant be served for data directly to the provider.

36. Additionally, your affiant requests specific permission of this court to search any person present in the areas designated for search, and to seize and search any and



C. J.

all digital media capable of receiving, transmitting, sending, or storing digital or electronic data, information, or files, if found in possession or under the control of any person. It is important to note that modern digital media with the aforementioned capabilities are smaller than in the past and are commonly carried on or about one's person. Examples of such devices are thumb drives, cell phones, iPods, and personal digital assistants (PDA)/Smartphones that are capable of accessing the internet (i.e. Blackberry, iPhone, Samsung Galaxy, etc.).

37. Your affiant would request that subsequent to the seizure of computer system components and any associated software documentation, as more specifically described in "Appendix A", that such evidence be transferred to a secure law enforcement location where its contents may be forensically examined in a manner best suited to retrieve and preserve all evidence. The alternative would be that law enforcement officers, in order to effectively execute the search warrant, would have to virtually move in and occupy the search premises for days or longer while the search proceeds. Operating in such a non-secure location for such duration would, in your affiant's opinion, endanger officer safety and significantly diminish the ability to fully retrieve and preserve evidence for which probable cause exists in the above-described computer system(s).

David J. Faucher, Sergeant
Shrewsbury Police Department

Then personally appeared the above-named David J. Faucher and made oath that the foregoing affidavit is true, this September 21, 2022:

Before me,

Justice/Clerk
District Court Department

# Appendix "A"
# Items to be Searched for

1. Any and all computer Systems, including, but not limited to:

   a. System components, including, but not limited to: the computer chassis, motherboard, CPU, memory, add-on boards, cables, and power supplies;
   b. Computer storage devices, removable storage devices and digital content, including, but not limited to:

      1. Floppy diskettes;
      2. Internal & external hard drives;
      3. Compact Discs, both read only & writeable (CD-ROM, CD-R, CD-RW);
      4. Digital Tapes;
      5. Zip/Jazz disks;
      6. VHS and VHS-like tapes;
      7. Digital Video Discs (DVD-ROM, DVD-R, DVD+R, DVD-RW, DVD+RW);
      8. PDAs (Personal Digital Assistants);
      9. MP3 Players;
      10. Digital Cameras;
      11. Cell Phones;
      12. Portable tablet computing devices; and
      13. Flash memory devices and/or flash memory cards.

   c. Input devices, including, but not limited to:
      1. Keyboards, mice, trackballs, pointers, etc.;
      2. Scanners, digital cameras, video capture cards, microphones, modems, etc.;
      3. Floppy Diskette Drives, Digital Tape Drives, Writable Compact Disk Drives, Writable Digital Video Disk (DVD) Drives;
      4. Zip/Jazz drives;
      5. Video cassette recorders.

   d. Output Devices, including, but not limited to:
      1. computer monitors;
      2. computer speakers;
      3. computer printers;
      4. Floppy Diskette Drives, Digital Tape Drives, Writable Compact Disk Drives, Writable Digital Video Disk (DVD) Drives;

   e. Network Devices, including, but not limited to:
      1. Cable/DSL modems;
      2. Wired/Wireless Routers; and
      3. Network cards.

2. Computer System Documentation, including, but not limited to, Operating System and Application programming disks and Programming and Application manuals, books or brochures.

# Appendix "A"
# Items to be Searched for

3. Computer software, hardware, and related items to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.

4. Items containing or displaying passwords, access codes, usernames, or other identifiers necessary to examine or access items, software, or information seized.

5. Any documents pertaining to the possession, receipt, origin, or distribution of images involving the exploitation of children.

6. Correspondence, items or other documents exhibiting an interest in the exploitation of children.

7. Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts to include credit card bills, telephone bills, correspondence, and other identification documents.

8. Items that would tend to show ownership and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements, and other identification documents.

9. Photographing and/or videotaping of the residence to be searched.

10. Visually explicit images/videos, whether on paper or its equivalent, which includes but not limited to negatives, slides, books, magazines, videotapes, photographs or other similar visual reproduction, or depiction by computer (specifically including such images/videos as stored within computer storage devices as computer data files) depicting any child known or reasonably believed to be under the age of 18 years of age, in which the child is:

    a. Actually or by simulation engaged in any act of sexual intercourse with any person or animal;
    b. Actually or by simulation engaged in any act of sexual contact involving the sex organs of the child and the mouth, anus or sex organs of the child and the sex organs of another person or animal;
    c. Actually or by simulation engaged in any act of masturbation;
    d. Actually or by simulation portrayed as being the object of, or otherwise engaged in, any act of lewd fondling, touching, caressing involving another person or animal;
    e. Actually or by simulation engaged in any act of excretion or urination within a sexual context;
    f. Actually or by simulation portrayed or depicted as bound, fettered, or subject to sadistic, masochistic, or sadomasochistic abuse in any sexual context; or
    g. Depicted or portrayed in any pose, posture or setting involving a lewd exhibition of the unclothed genitals, pubic area, buttocks or, if such person is female, a fully or partially developed breast of the child.

11. Authorizing officers to copy digital evidence stored on a server (or servers) in another location if a server can be remotely accessed from a computer (or computers), a tablet (or tablets), and/or a cell phone (or cell phones) located at the site authorized to be searched by this warrant. This authorization would permit law enforcement to preserve the integrity of such "cloud based" evidence and prevent it from being tampered with or destroyed.

12. Authorizing officers to secure the above computer related items and transport them to an off-

# Appendix "A"
# Items to be Searched for

site secure location, to continue the search of the computer items and computer storage devices for the following items:

a. Computer files, data, or other similar visual reproduction containing any sexually explicit visual images/videos or depiction by computer, of any child whom the person knows or reasonably should know to be under the age of 18 years of age and such child is:

i. Actually or by simulation engaged in any act of sexual intercourse with any person or animal;

ii. Actually or by simulation engaged in any act of sexual contact involving the sex organs of the child and the mouth, anus or sex organs of the child and the sex organs of another person or animal;

iii. Actually or by simulation engaged in any act of masturbation;

iv. Actually or by simulation portrayed as being the object of, or otherwise engaged in, any act of lewd fondling, touching, or caressing involving another person or animal;

v. Actually or by simulation engaged in any act of excretion or urination within a sexual context;

vi. Actually or by simulation portrayed or depicted as bound, fettered, or subject to sadistic, masochistic, or sadomasochistic abuse in any sexual context; or

vii. Depicted or portrayed in any pose, posture or setting involving a lewd exhibition of the unclothed genitals, pubic area, buttocks or, if such person is female, a fully or partially developed breast of the child.

b. Computer data files, records, logs associated with any of the above described files which may identify, trace, or record the facts, including but not limited to the date, time, modification, alteration, transmission or receipt via the Internet or other networks of any of the computer files described above, including, but not limited to file menus, Internet browser history, cache directories, registry entries, logs, and files.

c. Computer data files in the form of email, instant messaging, chat logs, or other communication logs, the contents of which involves the attempt to find, possess, acquire, store, or distribute child pornography.

d. Internet searches, stored within a computer file or data, using Internet search engines or file sharing programs for child pornography.

e. Any and all files associated with the installation, configuration and use of any peer to peer file sharing client, such as BitTorrent, uTorrent, Vuze, Ares, Shareaza, Bearshare, Limewire, etc...

f. Computer files and/or data that assist in identifying use, custody, control, or ownership of the computer systems and the removable storage devices.

g. Computer files and/or data that contain passwords, access codes, usernames, or other identifiers necessary to examine or access items, software, or information seized.

h. Computer data files and/or data containing the following terms:

# Appendix "A"
# Items to be Searched for

i. IP Address: **2600:1000:b0d:26ea:7416:ac90:5572:5306**

ii. Client Program: **Snapchat**

iii. Screen/username: **mikle888**

iv. Phone number: **774-253-5696**

v. Filename/MD5:

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~417-4c7eda5c4a.jpg
MD5: 3de3d44692a389668f0afce9475ab8a5

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~391-93dd7d7cd1.jpg
MD5: 93de5add6caf864088dfb1827ffc1998

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~386-cef3e00735.jpg
MD5: 15c129ea18afee22b2edd30bf5cb3e1d

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~424-3af52078f9.jpg
MD5: b0166e8fda6eb6620b55e63cb89186f0

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~422-a351862280.jpg
MD5: ca362cd2229d5dd0f3a0f265fd4755e9

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~447-0febc3eac6.jpg
MD5: 2f4f485d00f12d5eb4d642d66347494f

# Appendix "A"
# Items to be Searched for

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~443-1d15d00e88.jpg
MD5: 63db5d40e4484f87e01179c1c6c3d20f

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~331-1fd3f85c3b.jpg
MD5: 298528873888841195fa2e8ad9137781

Filename: mikle888-None-1044d045-51ec-5ddd-8cc0-c819f285df78~157-500747a6f3.jpg
MD5: 8f6d98a7517ac3cb8deab8333c104516

# Exhibit 1

Based on my training, experience, and conversations with other investigators with whom I have worked with and have participated in computer/Internet investigations, I know the following regarding the seizure and searching of computer evidence:

A. Computers can exist as a "stand alone" computer or as a "networked computer". A "stand alone" computer is one that is isolated from or not attached to any other computer. A "stand alone" computer is becoming rarer in today's high tech interconnected world. A "networked computer" is one that is connected to, attached to, or can communicate with other computers or hosts. "Networked computers" can share computer services with other computers such as file sharing, file storage, remote administration, email, printing and many more services. For example, a computer in a home may have a printer attached to it. Other computers on the home network can print to that printer because the host computer is sharing that resource. Most computers today have the ability to become networked, even temporarily, when they attach to the internet through a dial up modem.

B. A stand alone "computer system" is sometimes referred to as a work station, personal computer, or laptop and generally is composed of two parts; hardware and software. The hardware components can generally be broken down into four common categories: 1) system components; 2) data storage devices; 3) input devices; and 4) output devices. The software can be broken down into two categories: 1) operating systems; and 2) application software. Computer software are the tools that allow a user to produce data files, which are usually stored on the computer's data storage devices.

C. The system components are generally installed inside a case or chassis. They include, but are not limited to, the system board, central processing unit (CPU), random access memory (RAM), read only memory (ROM), cache memory, add on boards, and a power supply. The most important computer system component is the system board, commonly referred to as the "motherboard". It is an electronic circuit board that all other circuit boards or other electronic devices plug into. The "CPU" or central processing unit is the brain of the computer. Its function is to organize the requested actions received from the components. The processor receives requests, determines what tasks the computer needs to perform to fulfill those requests, and translates those tasks into electronic signals that the required devices can understand. The processor does the math and logical calculations. The processor is plugged into the motherboard.

D. Memory can take various forms including RAM, ROM, and Cache. The most common is Random Access Memory or RAM. RAM is used to temporarily store instructions and data that the CPU will need. The information in RAM is very volatile and is constantly being read, written, changed, and removed. When power to the computer is lost, all the information in RAM is lost as well. ROM is Read

Only Memory. ROM is usually a computer chip installed on the mother board that has computer instructions or data permanently imprinted on it. Cache memory is usually a memory chip installed on the CPU or very close to the CPU. It is usually much faster for the CPU to read the Cache memory than it is to read the Random Access Memory. Because memory is volatile and information will be lost when the computer loses power, information that is evidentiary in nature that is in memory will be lost as well. Therefore, it may be necessary for the investigator to perform some processing to secure the information in RAM prior to the computer being powered down. An example would be a word processing document that has not yet been saved or the current state of the computer's network connections.

E. Probably the most important components of a computer system, to a criminal investigator, are the computer's storage devices. Storage devices is a technology that is changing at an extremely fast pace both in terms of the type of storage devices available and the quantity of data the storage devices are capable of holding. The storage device holds or stores information or data, even when the computer's power is turned off. The data stored on the storage devices are kept unless they are manually removed or altered by the user or the computer's software. Often computer systems have multiple storage devices. Traditionally these storage devices were hard drives that were installed inside of a computer case. They were attached to the computer's mother board by cables referred to as ribbon cables and were powered from the computer's internal power supply. Today, internally installed hard drives are still a major component of a computer system. However, the availability and popularity of external hard drive storage devices or enclosures is growing rapidly. These external hard drive devices have become more ready available to the consumer over the past few years. New technologies, such as USB, Fire wire, and wireless connectivity allow data transfer rates between the computer and the hard drive at speeds that were not previously possible. These hard drives work the same way as the internal hard drives. What makes them different is that they are external to the computer and therefore removable and portable. These removable hard drive storage devices allow a user to plug the device into a computer system, read from or write to the device, and then unplug the device and store it somewhere away from the computer. These storage devices can be used to back up files that are important to the user. It could also be used to move files from one computer to another. A user could plug the device into a computer at work, copy files to the removable storage media, bring the device home, attach it to the home computer, and copy the files to the home computer's hard drives. These devices therefore could be located almost anywhere within a home or business that is the subject of a search.

F. Removable storage devices are another area that is changing at a rapid pace and the criminal investigator needs to consider just how portable and small removable storage devices can be. Removable storage traditionally consisted of floppy diskettes. Floppy diskettes are still popular today. They are small removable storage devices that are placed inside of a floppy diskette drive. The amount of storage space is somewhat limited and is normally 1.44 megabytes on a 3.5 inch floppy diskette. The need for greater removable storage has lead to the development of different technologies. One of these technologies is compact disc or



e.f.

CD. Compact discs are storage devices that are capable of storing computer files and can generally store 650 MB of data. This is approximately 450 times more data than floppy diskettes. Compact Discs originally could only be read from and not written to. However, compacts discs have changed and now can be both read from and written to multiple times much like a floppy disk. Writeable compact discs are commonly referred to as CD-R and CD-R/W discs. Other portable storage solutions exist including USB portable storage devices, sometimes refetred to as "thumb drives". These are very small devices, most often smaller than a person's thumb, and can easily fit into a person's pocket. They plug into the computer's USB port and allow a user to store up to gigabytes of data. These devices today are being manufactured to look like normal everyday items, such as writing pens and wrist watches. Other types of removable or external storage devices are tapes and tape drives, Zip/Jazz drives and Zip/Jazz disks, digital video disc (DVD) drives and digital video discs (DVD, DVD-R, DVD+R, DVD-RW, and DVD+RW), and flash media. These removable media storage devices are portable and have the ability to store large amounts of data. They can be easily concealed and carried off in a shirt pocket.

**G.** Other digital devices, such a personal digital assistants (PDA), cellular telephones, MP3 players, and digital cameras all have the ability to store data, can be connected to a computer, and data can be transferred to or from the device and the computer. The presence of these storage devices needs to be considered during the search for digital evidence. Again, these devices can be very small and easily hidden. Although a MP3 player is made to store and play back MP3 audio files (usually music), it is a digital device and any type of file could be stored on it, including image files. The newest cellular telephones have the ability to access the internet, E-mail, send photo's, and are capable of having an extensive address book.

**H.** Computer "input" and "output" devices are commonly referred to as "computer peripherals" or "peripheral devices". They tend to be external devices (outside the computer's case), although connected in some manner to the computer system. These devices can be connected to the computer using a wired or wireless technology.

Input devices are devices that allow a user to input data or instructions into the computer system for processing. They commonly include keyboards, mice, scanners, digital cameras, modems, video capture cards, and microphones. Other less common "input devices" may also be present as part of a computer system, but are usually present to accomplish a specialized function, such as a joystick for computer games.

Output devices are components through which the computer sends or "outputs" data. The monitor is a visual device that displays the primary output of a computer. The printer is another important output device. It produces output in the form of paper often referred to as hard copy. Printers take a variety of forms including ink jet, laser and dot matrix printers. Computer speakers are an example of an output device that outputs the audio sound from the computer. Other less common "output devices" may be present as part of a computer system usually to accomplish a specialized function.



C.S.

Removable media drives can also be considered an Input and/or Output devices, including, but not limited to the following: 1) Digital Tape Drives, 2) Writeable Compact Disc Drives; 3) Writable Digital Video Disk (DVD) Drives; 3) Zip/Jazz drives; 4) Floppy Diskette Drives; and 5) Video cassette recorders.

I. The second category of a typical "computer system" is "software". Software typically is categorized into two general sub-categories: 1) operating system software; and 2) application software. In some instances, it is hard to make a distinction whether a program is part of the operating system or a separate application.

J. "Operating Systems" are software programs designed to instruct the computer how to "operate". These instructions control how the system will process data, run applications, and which hardware will function. There are many different operating systems. Common operating systems include products made by Microsoft Corporation, which include Windows 95, 98, ME, 2000, XP Home and XP Professional. There are hundreds of operating systems and variants, including, but not limited to DOS, Linux, FreeBSD, Macintosh, and UNIX. As operating systems mature they offer additional features. Many of the newer operating systems implement features that focus on security and privacy. As an example, an operating system can be configured to require a user name and password to gain access to the computer. Some operating systems have logs that keep track of both successful authorized logins, as well as attempted unauthorized logins that failed. In addition, operating systems may implement methods of storing data in more secure compressed, password protected, or encrypted formats. Computers installed in a home environment are less likely to have implemented security procedures than are computers in a business environment.

K. "Applications" are computer programs designed to be used by a user to perform some function or service for the user. Application software makes requests of the operating system to perform various tasks. There are many different types of application software. Common application programs' functions include spreadsheet, word processing, database, graphic design, accounting, web browsing, and e-mail. Other software applications are designed to protect, hide, securely delete, encrypt, compress, or password protect data. It is important to remember that software almost always has a legitimate purpose, which can include the security and privacy of a user's legitimate data. However, a person can also use this software to conceal, delete, or disguise records of illegal activities.

Software applications don't necessarily store the information in a human readable format on the hard drive. They store the information in a format that the program understands and the program, when asked, presents that data on an output device in a human readable format, such as on a computer monitor or printer.

L. Networked computers are one or more stand alone computers that have the ability to communicate with each other. In order to communicate with another computer a computer must have some physical device to allow the communication to occur. These devices include but are not limited to modems, network cards, or wireless network cards. Today more and more people have small networks in their



C.S.

homes. This may be two or more computers connected together to share a printer or internet connection.

A wireless network card allows a computer to communicate to another computer via the radio spectrum; much like a cordless telephone allows a user to move around their house with a telephone.

M. A modem is a physical device that may either be installed within or attached to a computer system. A modem allows a computer to call another computer that also has a modem using traditional telephone lines. A network card is a physical device installed either inside or external to the computer and allows the computer to be connected to another computer via a wire or cable of some type. An example would be in a business environment where a user's workstation is attached to a server. Common today in homes are both Cable modems and DSL modems. These allow users to have much faster connections to the internet than was provided by a dial up telephone connection. The Internet Service Providers (ISPs) in these cases are cable TV companies or telephone companies. In addition, these types of connections can be "always on". Since there is no dialing involved, a user can be always connected.

N. Every computer that communicates over the Internet is assigned an Internet Protocol (IP) address that uniquely identifies the device and distinguishes it from other computers on the Internet. An IP address consists of 32 bits, often shown as 4 octets of numbers from 0-255 represented in decimal form instead of binary form. An example of an IP address is: "172.149.211.94" (without quotes). An IP address can be the same every time one connects (called a static IP address) or different per Internet session (called a dynamic IP address). The majority of IP addresses assigned to Internet Service Provider (ISP) customers are dynamic. Normally, when a user connects to the Internet, the user will first connect to an Internet Service Provider (ISP) such as AOL, MSN, RoadRunner, Adelphia Cable, UUNET, etc... via a telephone modem, cable modem, or DSL modem. The user is assigned a unique IP address by the ISP, which usually owns a range of IP addresses to be distributed randomly to it's customers. The user can then access the Internet in order to use services such as the World Wide Web, E-mail, Instant Messaging, etc... When the user disconnects from the ISP, if the IP Address is dynamic, the IP address then becomes available to be assigned to another user. I know that the majority of ISPs keep logs of IP addresses being assigned to users on a specific date and time.

The key issues are the following: 1) Only one user can be assigned a specific IP address at any given time while accessing the Internet; and 2) It is possible to identify the user that was assigned a specific IP address at a specific date and time through information maintained and provided by an Internet Service provider.

O. In a "Networked Computer" environment, a computer can offer services to a requesting computer. One of the services offered may be data storage services. This allows a user to store or retrieve data from or to a computer that could be hundred or thousands of miles away. The user in today's world no longer needs a file or program to be stored locally (on the user's own hard drive). They can run the program and then retrieve, read, write to, or store a file many miles away, even in a foreign country. Network storage services are prevalent on the internet today.

**P.** A computer system is an integrated system. Therefore, it is necessary to have all elements of that system in order to accurately retrieve and preserve evidence contained on that system. It is sometimes difficult, if not impossible, if you do not have the original hardware. As an example, one of the processes used by computer forensic personnel is to make an exact copy of the subject hard drive onto another hard drive. This copy could, with some older operating systems be placed inside of a different computer and it would start up fine. However, with today's operating systems, there are hardware and software conflicts that prevent this copy drive from operating correctly inside of a foreign computer and the forensic examiner is forced to place the copy back into the original computer in order to boot or start the computer. As another example, a document or an image may have been created and saved using a particular version of a particular software to a particular format capable of only being reasonably outputted on the peripheral printer of that system. Because of the multiplicity of computer systems available and the almost limitless number of operating system and application software, attempting to retrieve and preserve evidence from a computer system without the computer on which it was generated or saved; will not only be unreasonably time consuming, but costly as well. More importantly, the use of any other computer system to retrieve or preserve evidence from a given computer system could, under certain circumstances, alter or affect the evidence itself, especially, the computer's record of a file's creation date, modification date, or deletion date.

The seizure of software manuals is necessary because of the vast quantity of software on the market. The forensic examiner can not possibly know each and every type of software available and the manuals may provide needed information. Computer users are also known to write down user names, passwords or access codes or other important information needed to gain access to the computer, to execute a program or to open a file, on paper or record them in some manner. It is necessary for the criminal investigator to search for items of this nature.

For these reasons, it is more reasonable to seize the entire computer system, all storage media, input and output devices, all software, and any documentation associated with that software. To do this work accurately and completely requires: 1) the seizure of all computer equipment and peripherals, which, may be interdependent; 2) the software to operate the computer system; and 3) the instructions manuals for the computer system and software programs.

**Q.** In addition, the search for computer storage devices and removable media needs to be extensive to be complete. As mentioned, the computer system itself is but one piece of the evidence. Storage media is small and can be easily hidden. Your affiant is familiar with situations where media has been hidden in drop ceilings.

**R.** The physical set up of the computer can be complicated with cables connecting different devices. It is necessary that the investigator accurately and completely document that state of the computer system. This documentation should include photographing all aspects of the computer system including, but not limited to, what is visible on the monitor at the time of the search, the cabling, the peripherals attached, and the overall physical location of the computer in the search location.



C.J.

S. In most circumstances it is not reasonable to perform the search of computer media at the search site itself. In order to properly retrieve and analyze all electronically stored data, to document and authenticate such data, and to prevent the loss of the data from accidental or deliberate programmed destruction, it requires off-site laboratory analysis by a qualified computer specialist. Several factors justify the off-site search of the computer media including but not limited to; the quantity of the storage media, the storage capacity of that media, the physical environment of the search area, the nature of digital evidence in general, the nature of the crime under investigation, the nature of the evidence sought, the time involved to complete the search, and the intrusion and the need to limit that intrusion or inconvenience to persons at the search site.

T. As already mentioned, the search for digital evidence may involve the seizure of multiple computers and a large quantity of removable media. The computer storage devices mentioned are capable of storing millions of pages of information. A "byte" is the equivalent of storing a single letter typed at the keyboard. A kilobyte (KB) is one thousand bytes, a megabyte (MB) is one million bytes and a gigabyte (GB) is one thousand megabytes. A 100 MB storage device would have the capacity of storing fifty thousand pages of typewritten, double spaced text. Many computer systems that are purchase today contain an 80 GB hard drive or larger. Additionally, one or more 300 GB hard drives can be purchased and installed internally or attached externally to a computer. These drives have the ability to store huge volumes of data. If a computer uses additional storage media (e.g. floppy diskettes, tapes, Zip/Jazz, writable CDs & DVDs, flash memory, etc.) the capacity for storage is limitless.

U. The size of a storage device is but one issue when it comes to locating a file or files that are the target of a search. The software used to create or store the file may be such that it is not conducive to finding it with keyword searching. As mentioned, software may save data in a proprietary format, in an encrypted or compressed format that is not humanly readable and therefore not conducive to key word searching. In addition, the user can take other steps that inhibit law enforcement from discovering the information that is the subject of the search. This includes, but is not limited to, renaming files or file extensions, using encryption or compression, password protecting files, or using software specifically designed to allow a user to hide the geometry of a drive, or to embed a file within another file or files. A user does not need extensive computer knowledge to perform these steps and software is readily available for free on the internet that will perform these steps for the user.

V. Most searches are performed in physical environments that are not favorable to proper methods of searching computers. The location itself may be limited in size. Computers require electrical power and many locations lack proper lighting and the availability of power. Search locations tend to be hostile in nature. The equipment brought to a scene to perform a search is expensive and can easily be broken. The controlled environment needed to perform an electronic search is most times not present at a search site.



C.d.

Furthermore, the nature of digital evidence in general effects the ability to perform a search onsite. Digital evidence is extremely sensitive and can be altered or destroyed by both intentional as well as unintentional acts. Software programs installed on the subject's computer can perform actions that are unanticipated or can be set to run at various dates and times that would alter or change the state of the computer and its storage devices. Computer evidence is extremely vulnerable to tampering or destruction, both from external sources and from destructive codes embedded in the system programs. It is necessary to perform searches in a more controlled environment. This includes the physical environment, as well as the hardware and software used to process the subject media.

W. The nature of the crime under investigation along with the type of evidence sought is important to consider. In a child pornography case, one of the important elements of that crime is knowledge of the nature and contents of the files. Simply finding child pornography on the storage media is not a thorough or complete enough search. Searching must be performed for evidence that can indicate how, when, and by whom a file was placed on the computer system. Who accessed the file, when was the file accessed and was the file sent to others? This type of information isn't clearly evident; the forensic examiner must review and analyze the various operating system and software configurations, the directory and folder structure, logs of computer activity, files created, modified, or accessed around or about the time the file of evidentiary value was created, modified, or accessed. From the information gathered, the forensic examiner must draw reasonable conclusions concerning who had knowledge of the nature and contents of files and when. The searching for these files and the analysis of the information in these files can take a substantial amount of time.

X. This requires that personnel executing the search warrant must examine all the stored data to determine which particular files are relevant and fall within the scope of the warrant. This search process can take weeks or months, depending on the volume and complexity of the data stored, and it would be impractical to attempt this kind of data search onsite. The intrusion to the home or business required to perform this type of searching onsite would be far more intrusive than removing the items to a secure controlled location to perform the search.

Y. The analysis of electronically stored data whether preformed on-site or in a laboratory or other controlled environments, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file folders or directories and the individual files they contain; opening or reading the first few lines of such files in order to determine their precise contents; scanning storage areas to discover and possibly recover deleted data, scanning storage areas for deliberately hidden files, performing electronic keyword searching through all electronic storage areas to determine whether these storage areas contain information related to the subject matter of the investigation and searching for associated files or data that would record information as to when the file was created, when it was last written to, when it was last accessed, and by whom.

Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Search



C.A.

protocols are designed to protect the integrity of the evidence, and to recover hidden, erased, compressed, password protected, or encrypted files.

**Z.** Deleted files can be undeleted. When most computers store data, the operating software tells the CPU to assign the data a "file" name (usually a pre-existing file name if it exists, or a name selected [inputted via keyboard] by the user) and sends the data to a storage medium, typically either the "hard drive" of the computer, a floppy diskette, or some other peripheral storage device such as a Zip/Jazz disks, tapes, or writable compact discs (CD-R/W, DVD+R/W, or DVD-R/W). In order to manage the inventory of all stored files, most operating systems also maintain a "File Allocation Table" (FAT) or something similar which tells the CPU where all data is stored. The names and actual locations of the data on the hard drive or other storage medium are recorded in the FAT each time a "file" is saved, accessed, modified, transferred or otherwise affected. When a file is "deleted" by a user, the computer does not in fact remove its data from the designated storage medium, but, instead, alters the FAT to indicate that the space previously consumed by that "deleted" data is now available to be overwritten with new data if necessary. Typically, space that is consumed by "deleted" data is not overwritten until all other unconsumed space is first written to or consumed (although this factor may be affected by the type of the operating system and application software used). This fact is important in law enforcement since it means that so-called "deleted" files or data are, in fact, often still present on the computer's storage medium (i.e. floppy diskette, hard drive, tapes, etc.) and can be (and have been) recovered months, even years, after their deletion if the integrity of the computer system is maintained. In my experience, it is not at all uncommon to be able to "undelete" deleted files or data years after their deletion date. As the capacity of computers to store data rises each year, the likelihood that previously "deleted" data has not yet been overwritten and is still recoverable also rises concurrently. The result is that evidence of a crime, stored in a computer system, may be recovered even after the passage of significant periods of time and, in some instances, even after a deliberate attempt to destroy it. Furthermore, it is possible to determine when the file(s) were deleted and what physical location and logical directory they resided prior to their deletion.

**AA.** In the vast majority of computer systems, each time a file is received, transferred, modified, altered, or otherwise affected, the computer will make some form of a notation or record of that event either within the file properties themselves, in a "log" of activity, or by creating or modifying (at or about the same moment in time) a file "associated" with the computer data file which witnessed the activity. For example, when files are received in most IBM-compatible systems using Microsoft's Internet Explorer as a software application to navigate the Internet, the file is loaded into a "Temporary Internet" directory and/or "cache" files, and the Internet address of the source of the file is logged or recorded into the "navigation" directories and files of Microsoft's Internet Explorer. At the same time, if a computer system contacts an Internet Website, the Website itself may transmit a "cookie" which is short computer code which (using Microsoft's Internet Explorer as an example) is logged or recorded in the "Cookies" directory of the Internet browsing software. A "cookie" is a computer code logged into a receiving computer for future reference the next time that computer system contacts the Website. The



C.J

use of cookies is widely used and enables the Website administrator/owner to know if that computer system has previously visited the Website. Generally speaking, these cookies and cache files are computer data files which are "associated" with the computer data file containing the image or data being uploaded to or downloaded (transmitted) from the Internet to a computer accessing a website on the Internet. Just as a card index system may be created to catalog a limitless number of features relative to the contents of a filing cabinet, so too may "associated" computer data files be created for a wide variety of software applications relative to other computer data files (and not just merely Internet communication and browsing). This recording and logging feature is not limited to IBM-compatible computers. It applies to various computer systems and computer programs, although the name for the storage locations (e.g. "cache" or "cookie" file) may change depending on the computer system and the computer software. Through a careful and thorough analysis of files which are in any way "associated" with a file of evidentiary significance, it is possible to identify:

1. Where a computer system has "gone" or "visited" on the Internet;
2. Where certain evidentiary computer data files were taken from the Internet;
3. Who was at the keyboard at or around the time that certain computer data files of evidentiary significance were created, modified, printed, or deleted (e.g. The downloading of images from a child pornography Internet site might be immediately followed by a visit to the website of an employer); and
4. When the computer activity occurred.

**BB.** Computers are capable of disguising or hiding data to hinder its detection. Computers are capable of encrypting data so as to make it un-rettievable by the average computer user. The Massachusetts State Police has access to computer software which is available to law enforcement and which will assist in breaking some forms of encryption, but the use of such software can be time consuming, depending upon the amount of data stored and the complexity of the encryption. Attempting to decrypt data is an extremely time and equipment intensive process requiring a laboratory environment to be done effectively. Some users will purposefully rename files with otherwise innocuous file names or file extensions to deter curiosity seekers and others. Similarly, computer users may also "booby-trap" their computers or password protect their computer systems in an attempt to hide their activities and prevent the collection of evidence against them.

**CC.** That computer users frequently "back up" copies of hard drives, software, and data files onto computer storage media to guard against loss if their computer malfunctions; they keep those backup copies at their residence and other locations they have access.

**DD.** That a computer system's hard drive or other removable computer storage media will contain physical, electronic, optical, and/or magnetic evidence, both in files and data located in unallocated (unconsumed) space or slack space, which will aid in establishing the circumstances under which the crime was committed and/or



a.f.

which in general will assist in the discovery of the pertinent facts; and that such evidence requires a systematic search to locate, seize, record and process.

EE. For the purposes of this affidavit the terms "records", "documents", "materials" and "files" include all information preserved in any form – visual, magnetic, electronic or aural – including the originals and all non identical copies thereof, whether different from the original by reason of notations made on such copies or otherwise (i.e. a user creating a word document may have created different drafts prior to finalizing the document, a user may alter an image from it's original state, etc....). These definitions apply regardless of the form in which such records, documents, materials, files may have been created or stored, including but not limited to any handmade form (such as writing, drawing, or painting, with any implement on a surface, directly or indirectly); photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (such as writing, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, or any information on electronic or magnetic storage device, such as floppy diskettes, hard disks, CD/DVD Rom/Writeable discs, flash memory cards, PDAs, digital cameras, MP3 players, Zip/Jazz disks, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

# Exhibit 2