No. 22-4242

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

ZACKARY ELLIS SANDERS,

Defendant-Appellant,

v.

UNITED STATES OF AMERICA,

Plaintiff-Appellee.

Appeal from the United States District Court
for the Eastern District of Virginia (No. 1:20-cr-00143-TSE)

JOINT APPENDIX VOLUME 3 OF 8 (JA892–JA1371)

William G. Clayman
Aidan Taft Grano-Mickelsen
UNITED STATES ATTORNEY'S OFFICE
FOR THE EASTERN DISTRICT OF VIRGINIA
2100 Jamieson Avenue
Alexandria, VA 22314
Telephone: (703) 299-3744
william.clayman@usdoj.gov

Counsel for Appellee

Lawrence S. Robbins
Brandon L. Arnold
Leslie C. Esbrook
KRAMER LEVIN ROBBINS RUSSELL
2000 K Street NW, 4th Floor
Washington, D.C. 20006
Telephone: (202) 775-4500
lrobbins@kramerlevin.com

Counsel for Appellant

TABLE OF CONTENTS

VOLUME 1

E.D. Va. Docket Sheet (No. 1:20-cr-00143-TSE) JA1

Affidavit in Support of a Criminal Complaint and an Arrest Warrant (March 19, 2020) (Dkt. 4) JA61

Government's Response in Opposition to Defendant's Motion for Revocation of Detention Order (April 1, 2020) (Dkt. 15) JA74

Indictment (June 24, 2020) (Dkt. 29) JA86

Order (August 21, 2020) (Dkt. 74) JA92

Exhibit 1 to [Dkt. 97] Government's Omnibus Response in Opposition to Defendant's Motions to Suppress: Cox Communications' response (Dkt. 97-1) JA93

Exhibit 2: Transcript of motion hearing, *United States v. Bosyk*, 1:17-cr-302 (E.D. Va. Feb. 2, 2018) (Dkt. 97-2) JA97

Order (October 26, 2020) (Dkt. 114) JA104

Unopposed Motion to Continue Trial and Waiver of Speedy Trial Rights (October 28, 2020) (Dkt. 116) JA105

Renewed Unopposed Motion to Continue Trial and Waiver of Speedy Trial Rights (October 30, 2020) (Dkt. 124) JA109

Government's Notice of Intent to Present Evidence Under Federal Rule of Evidence 414 (November 2, 2020) (Dkt. 127) JA115

Government's Amended Notice of Intent to Present Evidence Under Federal Rule of Evidence 414 (November 17, 2020) (Dkt. 133) JA121

Memorandum in Support of Motion to Suppress Statements (December 17, 2020) (Dkt. 150) JA127

Exhibit 1: February 14, 2020 FD-302 Report (Dkt. 150-1) JA148

Exhibit 2: Declaration of Dr. Risa Sanders (Dkt. 150-2) JA152

Exhibit 3: Excerpts of Transcript of Zackary Sanders's February 12, 2020 Recorded Statement (Dkt. 150-3) JA162

Order (December 18, 2020) (Dkt. 152) JA205

Memorandum in Support of Motion in Limine in Opposition to Government's Amended Notice of Intent to Present Evidence Under Federal Rule of Evidence 414 (December 18, 2020) (Dkt. 154)..... JA207

Government's Motion *in Limine* to Exclude and Limit Certain Arguments, Lines of Questioning, and Evidence at Trial (December 18, 2020) (Dkt. 163)..... JA215

Government's Motion *in Limine* to Introduce Certain Evidence Pursuant to Federal Rules of Evidence 404(b) and 414 (December 18, 2020) (Dkt. 165)..... JA231

Government's Response in Opposition to Defendant's Motion to Compel (December 18, 2020) (Dkt. 167)..... JA248

Defendant's Response to Show Cause Order (December 23, 2020) (Dkt. 177)..... JA269

Government's Position on the Court's Order to Show Cause (December 29, 2020) (Dkt. 179) JA278

Order (January 7, 2021) (Dkt. 196) JA288

United States' Response to Defendant's Motion *in Limine* in Opposition to Notice Pursuant to Federal Rule of Evidence 414 (January 8, 2021) (Dkt. 201)..... JA295

Opposition to Government's Motion in Limine to Introduce Evidence Pursuant to Federal Rules of Evidence 404(b) and 414 (January 8, 2021) (Dkt. 207)..... JA304

Defendant's Renewed Motion for Leave for this Court to Consider His Motion to Suppress Statements as Timely Filed (January 13, 2021) (Dkt. 213)..... JA313

Order (January 14, 2021) (Dkt. 214) JA319

Reply to Government's Response to Mr. Sanders's Opposition to 414 Notice (January 14, 2021) (Dkt. 216)..... JA320

Reply to Defendant's Response to Motion *in Limine* to Admit Certain Evidence Pursuant to Federal Rules of Evidence 404(b) and 414 (January 15, 2021) (Dkt. 223)..... JA327

Reply to Defendant's Response to Motion *in Limine* to Exclude and Limit Certain Arguments, Lines of Questioning, and Evidence at Trial (January 15, 2021) (Dkt. 224)..... JA332

Mr. Zackary Ellis Sanders's Notice of Supplemental Authority in Support of His Opposition to Government's Motion *in Limine* to Exclude and Limit Certain Arguments, Lines of Questioning, and Evidence at Trial (January 18, 2021) (Dkt. 225) JA338

Notice of Correction (January 21, 2021) (Dkt. 232) JA342

Government's Response to Defendant's Motion for Leave to File Untimely Fifth Motion to Suppress (January 22, 2021) (Dkt. 235) JA345

Defendant's Reply to Government's Opposition to His Renewed Motion for this Court to Consider His Motion to Suppress Statements as Timely Filed (January 29, 2021) (Dkt. 243) JA354

Order (February 4, 2021) (Dkt. 245) JA361

Defendant's Notice of Objection to Rule 404 and 414 Ruling (May 10, 2021) (Dkt. 337) JA364

Government's Response in Opposition to the Defendant's Fourth Motion to Compel (May 14, 2021) (Dkt. 350) JA368

Order (May 26, 2021) (Dkt. 369) JA374

Zackary Ellis Sanders's Renewed Motion to Suppress Statements Taken in Violation of *Miranda v. Arizona* (August 19, 2021) (Dkt. 429) JA382

Memorandum in Support of Renewed Motion to Suppress Statements Taken in Violation of *Miranda v. Arizona* (August 19, 2021) (Dkt. 430) JA385

Government's Response in Opposition to Defendant's Second Renewed Motion to Reconsider His Motion to Compel (August 19, 2021) (Dkt. 432) JA390

Order (August 25, 2021) (Dkt. 442) JA399

Government's Response in Opposition to Defendant's Second Renewed Motion to Reconsider the Court's Denial of Defendant's Fifth Motion to Suppress as Untimely (August 30, 2021) (Dkt. 446) JA401

Order (September 8, 2021) (Dkt. 457) JA409

Curriculum vitae of Dr. Fred S. Berlin (October 4, 2021) (Dkt. 480-1) JA411

Government's Response in Opposition to Defendant's Motion to Reconsider His Motion to Suppress (October 8, 2021) (Dkt. 490) JA448

VOLUME 2

Reply to the Government's Opposition to Mr. Sanders's Renewed Motion to Suppress Based on the Warrantless Use of a Network Investigative Technique and False Material Information in Affidavit Paragraph 25 (October 12, 2021) (Dkt. 491) JA458

Defendant Zackary Ellis Sanders's Supplemental Proposed Jury Instructions (October 14, 2021) (Dkt. 500) JA464

Order (October 13, 2021) (Dkt. 501) JA512

Order (October 21, 2021) (Dkt. 522) JA515

Defendant's Objection to Court's Jury Instruction Regarding "Consent Is Not a Defense" and the Exclusion of Evidence Demonstrating Assent (October 25, 2021) (Dkt. 529) JA518

Order (October 25, 2021) (Dkt. 530) JA525

Defendant's Notice of Filing of Objection to Jury Instruction Regarding His Purpose (October 25, 2021) (Dkt. 534) JA529

Government's Revised Trial Exhibit List (October 27, 2021) (Dkt. 539-2) JA534

Motion for Enlargement of Time in Which to File Motion for a New Trial Under Federal Rule of Criminal Procedure 33 and/or Motion for Judgment of Acquittal Under Rule 29 and Memorandum in Support (November 4, 2021) (Dkt. 543) JA547

Transcript of Trial Day 7 (October 27, 2021)[1] (Dkt. 551) JA550

Transcript of Trial Day 1 (October 19, 2021) (Dkt. 552) JA616

Transcript of Pretrial Conference (October 15, 2021) (Dkt. 555) JA774

Public Exhibits to [Dkt. 586] Memorandum in Support of Motion for New Trial

Exhibit 6: Motion to Suppress Evidence, *United States v. Bateman*, No. 1:20-cr-10012-IT (D. Mass. Dec. 27, 2021) (Dkt. 586-6) JA839

[1] The captions of the trial transcripts incorrectly show the trial dates as having occurred in November 2021.

VOLUME 3

Exhibit 9: Application for a Search Warrant, *In the Matter of the Search of Property of* [redacted], *Pleasant Garden, NC 27313*, No. 1:20-mj-243-LPA (M.D.N.C. Aug. 18, 2020) (Dkt. 586-9).....JA892

Exhibit 10: Application for a Search Warrant, *In the Matter of the Search of* [redacted], *Burlington, VT*, No. 2:20-mj-00143-KJD (D. Vt. Dec. 4, 2020) (Dkt. 586-10).....JA976

Exhibit 11: Application for a Search Warrant, *In the Matter of Search of Premises Located at* [redacted], *Barnhart Missouri, 63012*, No. 4:20-MJ-3301-NCC (E.D. Mo. Nov. 12, 2020) (Dkt. 586-11).....JA1021

Exhibit 12: Affidavit in Support of Search Warrant, *In the Matter of the Search of* [redacted], *Chipley, Florida 32428*, No. 5:20-mj-44-MJF (N.D. Fla. May 6, 2020) (Dkt. 586-12).....JA1058

Exhibit 13: Application for a Search Warrant, *In the Matter of the Search of Entire property located at* [redacted]., *Gardiner, Maine 04345*, No. 1:20-mj-00255-JCN (D. Me. Sept. 8, 2020) (Dkt. 586-13).....JA1122

Exhibit 14: Application for a Search Warrant, *In the Matter of the Search of the premises known as* [redacted], *Rochester, NH*, No. 1:21-mj-00146-AJ (D.N.H. June 4, 2021) (Dkt. 586-14).....JA1163

Exhibit 15: Affidavit in Support of Search Warrant, *In the Matter of Search at* [redacted], *Lansing, Michigan 48912*, No. 1:20-mj-00481-SJB (W.D. Mich. Nov. 19, 2020) (Dkt. 586-15).....JA1196

Exhibit 17: 01/13/2017 FD-302 (Dkt. 586-17).....JA1230

Exhibit 39: Operation H Statistics (Dkt. 586-39).....JA1232

Exhibit 41: 03/02/2022 Press Release (Dkt. 586-41).....JA1236

Exhibit 42: 03/01/2022 Press Release (Dkt. 586-42).....JA1241

Exhibit 43: 03/02/2022 Press Release (Dkt. 586-43).....JA1247

Government's Response in Opposition to Defendant's Motion for New Trial and to Reconsider Motions to Compel and Suppress (March 18, 2022) (Dkt. 593).....JA1251

Exhibit 1: Order on Motion for Discovery, *United States v. Kiejzo*, No. 20-40036 (D. Mass. Oct. 4, 2021) (Dkt. 593-1) JA1266

Notice of Filing of Supplemental Exhibits (March 22, 2022) (Dkt. 599) JA1278

Exhibit 1: Affidavit in Support of Application for Issuance of a Criminal Complaint, *United States v. Holmstedt*, No. 2:21-cr-00004 (E.D. Va. Dec. 8, 2020) (Dkt. 599-1) JA1283

Exhibit 2: Statement of Facts, *United States v. Holmstedt*, No. 2:21-cr-00004 (E.D. Va. Feb. 4, 2021) (Dkt. 599-2) JA1289

Judgment (April 1, 2022) (Dkt. 621) JA1295

United States' Notice of Filing of Redacted Memorandum Opinion and Proposed Restitution Order (April 8, 2022) (Dkt. 627) JA1302

Notice of Appeal (April 13, 2022) (Dkt. 636) JA1306

Government Trial Exhibits 102A, 103A, 104A, 105A, and 106A: Redacted Transcript of Interview of Zackary Ellis Sanders (February 12, 2020) JA1309

Government Trial Exhibits 201 to 235: Photographs JA1337

VOLUME 4

FILED UNDER SEAL

Motion to Compel Discovery (July 13, 2020) (Dkt. 38) SJA1372

Exhibit 1: Declaration of Dr. Matthew Miller (July 12, 2020) SJA1393

Exhibit 2: FLA Intelligence Report SJA1405

Exhibit 3: FLA Letter SJA1407

Government's Response in Opposition to Defendant's Motion to Compel Discovery (July 27, 2020) (Dkt. 43) SJA1409

Exhibit 1: Search Warrant Affidavit (Dkt. 43-1) SJA1431

Reply to Government's Opposition to Motion to Compel Discovery (Dkt. 48) (July 30, 2020) SJA1473

Exhibit 1: 1/17/2020 FD-1057 Form (Dkt. 48-1) SJA1499

Exhibit 2: Second Declaration of Dr. Miller (Dkt. 48-2) SJA1504

Exhibit 3: Screenshot Taken by FBI of Posting on Page of Target Website (Dkt. 48-3) SJA1508

Exhibit 4: Declaration of Matthew Ryder, QC (Dkt. 48-4).....SJA1510

Government's Supplemental Brief in Opposition to Defendant's Motion to Compel Discovery (August 10, 2020) (Dkt. 57).....SJA1523

Supplemental Brief on Defendant's Motion to Compel Discovery (August 10, 2020) (Dkt. 58).....SJA1531

Exhibit 1 to [Dkt. 57] Government's Supplemental Brief in Opposition: FLA – Intelligence Report (Dkt. 59).....SJA1543

Exhibit 2: Declaration of Special Agent Christopher A. Ford (Dkt. 59-1).....SJA1545

Response to Government's Supplemental Brief on Defendant's Motion to Compel Discovery (Dkt. 65) (August 12, 2020).....SJA1551

Exhibit 1: Third Declaration of Dr. Matthew Miller (Dkt. 65-1).....SJA1560

Reply to Defendant's Response to Government's Supplemental Brief in Opposition to Defendant's Motion to Compel Discovery (Dkt. 70) (August 19, 2020).....SJA1563

Memorandum Opinion (August 21, 2020) (Dkt. 73).....SJA1568

Government's Response in Opposition to Defendant's Motion for Reconsideration of His Motion to Compel (September 9, 2020) (Dkt. 100).....SJA1582

Government's Omnibus Response in Opposition to Defendant's Motions to Suppress (September 9, 2020) (Dkt. 101).....SJA1590

Mr. Zackary Ellis Sanders's Reply to the Government's Opposition to His Renewed Motion to Compel (September 10, 2020) (Dkt. 105).....SJA1621

Mr. Zackary Ellis Sanders's Reply to the Government's Omnibus Opposition to Mr. Sanders's Motions to Suppress (September 10, 2020) (Dkt. 106).....SJA1628

Order (September 10, 2020) (Dkt. 107).....SJA1650

Memorandum Opinion (October 26, 2020) (Dkt. 113).....SJA1660

Memorandum in Support of United States' Motion to Seal, Keep Memorandum Opinion Under Seal, and File Redacted Memorandum Opinion (October 29, 2020) (Dkt. 121).....SJA1678

Mr. Zackary Ellis Sanders's Motion to Compel the Government to Produce Material, or, in the Alternative, to Submit Material for *In Camera* Inspection (November 27, 2020) (Dkt. 137).....SJA1685

Exhibit 1: Transcript of September 11, 2020 Hearing (Dkt. 137-1) SJA1709

Supplement to Motion to Compel (December 5, 2020) (Dkt. 140).....SJA1745

Defendant's Reply to the Government's Opposition to Motion to Compel the Government to Produce Material, or, in the Alternative, to Submit Material for *in Camera* Inspection (December 23, 2020) (Dkt. 176).....SJA1753

Exhibit 1: Target Website Homepage (Dkt. 176-1) SJA1776

Exhibit 2: Fifth Declaration of Dr. Matthew Miller (Dkt. 176-2).....SJA1778

Exhibit 3: Third Declaration of Matthew Ryder QC (Dkt. 176-3).....SJA1781

Exhibit 4: Target Website Page (Dkt. 176-4).....SJA1787

Exhibit 5: May 8, 2020 Letter (Dkt. 176-5) SJA1789

Exhibit 6: June 8, 2020 Letter (Dkt. 176-6) SJA1793

Exhibit 7: June 22, 2020 Letter (Dkt. 176-7) SJA1809

Exhibit 8: July 7, 2020 Letter (Dkt. 176-8).....SJA1818

Exhibit 9: July 27, 2020 Email (Dkt. 176-9).....SJA1824

Defendant's Reply to Government's Position on Order to Show Cause (January 4, 2021) (Dkt. 185).....SJA1827

Order (January 26, 2021) (Dkt. 236) SJA1833

Supplement to Defendant's Motion to Compel the Government to Produce Material, or, in the Alternative, to Submit Material for *in Camera* Inspection (January 26, 2021) (Dkt. 241).....SJA1841

Exhibit 1: Target Website Page (Dkt. 241-1).....SJA1851

Exhibit 2: Target Website Page (Dkt. 241-2).....SJA1853

Exhibit 3: January 22, 2021 Discovery Letter (Dkt. 241-3).....SJA1855

Exhibit 4: January 25, 2021 Email (Dkt. 241-4) SJA1878

Memorandum in Support of Mr. Zackary Ellis Sanders's Motion to Suppress Due to Lack of Probable Cause (Motion to Suppress No. 1) (September 2, 2020) (Dkt. 252).....SJA1880

VOLUME 5

FILED UNDER SEAL

Exhibit 1: Affidavit in Support of Application for Search Warrant (Dkt. 252-1).....SJA1898

Exhibit 2: List of FBI Agents Executing Warrant (Dkt. 252-2).....SJA1940

Exhibit 3: Description of 427 Photos Taken of Sanders Home (Dkt. 252-3).....SJA1944

Memorandum in Support of Mr. Zackary Ellis Sanders's Motion to Suppress Based on False and Misleading Material Information in Affidavit Paragraph 23 (Motion to Suppress No. 2) (September 2, 2020) (Dkt. 253).....SJA1959

Exhibit 1: FLA Intelligence Report (Dkt. 253-1).....SJA1993

Exhibit 2: September 16, 2019 FLA Letter (Dkt. 253-2).....SJA1995

Exhibit 3: FLA Intelligence Report (Dkt. 253-3).....SJA1997

Exhibit 7: Fourth Declaration of Dr. Matthew Miller (Dkt. 253-6).....SJA1999

Exhibit 8: Declaration of Seth Schoen (Dkt. 253-7).....SJA2009

Exhibit 9: Screenshot of Post Described in Paragraph 16 Taken by FBI in January 2019 (Dkt. 253-8).....SJA2034

Exhibit 10: Additional Screenshots Taken by FBI in January 2019 (Dkt. 253-9).....SJA2036

Exhibit 11: Search Warrant (Dkt. 253-10).....SJA2040

Exhibit 13: July 31, 2020 Hearing Transcript (Dkt. 253-12).....SJA2048

Memorandum in Support of Mr. Zackary Ellis Sanders's Motion to Suppress Based on False and Misleading Material Information in Affidavit Paragraph 25 (Motion to Suppress No. 4) (September 2, 2020) (Dkt. 254).....SJA2084

Exhibit 3: Affidavit in Support of Application for Search Warrant (Dkt. 254-3).....SJA2108

Exhibit 8: Second Declaration of Matthew Ryder QC (Dkt. 254-8).....SJA2150

Exhibit 9: Declaration of Dr. Richard Clayton (Dkt. 254-9).....SJA2155

Exhibit 10: Affidavit in Support of Application for Search Warrant, *In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion*, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015) (Dkt. 254-10).....SJA2173

Exhibit 11: Comparison Report of *Matish* Affidavit and *Sanders* Affidavit (Dkt. 254-11 to Dkt. 254-12).....SJA2208

Exhibit 12: Declaration of Special Agent Christopher A. Ford (Dkt. 254-13).....SJA2262

Memorandum in Support of Mr. Zackary Ellis Sanders's Renewed Motion to Compel Discovery or in the Alternative for Reconsideration of the Court's Order Denying His Motion to Compel (September 2, 2020) (Dkt. 255).....SJA2268

Mr. Zackary Ellis Sanders's Memorandum in Support of Motion to Suppress Based on Materially Misleading Statements and Omissions Regarding Tor, the Target Website, and the Subject Premises (Motion to Suppress No. 3) (September 2, 2020) (Dkt. 256).....SJA2279

Exhibit 5: Second Declaration of Dr. Matthew Miller (Dkt. 256-5).....SJA2309

Exhibit 9: Screenshot of Target Website (Dkt. 256-9).....SJA2313

Exhibit 10: Additional Screenshots Taken by FBI in January 2019 (Dkt. 256-10).....SJA2315

Corrected Memorandum in Support of Defendant's Motion to Continue Trial, and Waiver of Speedy Trial Rights (March 24, 2021) (Dkt. 270).....SJA2319

Defendant's Second Supplement to Corrected Motion to Continue Trial, and Waiver of Speedy Trial Rights (April 1, 2021) (Dkt. 282).....SJA2333

Memorandum in Support of Defendant's Motion for Leave to File Rule 12.2(b) Notice of Expert Evidence of a Mental Condition Bearing on Lack of Guilt (April 26, 2021) (Dkt. 305).....SJA2337

Government's Response to the Defendant's Motion for Leave to File Rule 12.2(b) Notice (May 5, 2021) (Dkt. 314).....SJA2342

Exhibit 1: March 30, 2021 Email (Dkt. 314-1).....SJA2349

Defendant's Memorandum in Support of Motion to Compel, or, in the Alternative, to Submit Material for *In Camera* Inspection (May 6, 2021) (Dkt. 335).....SJA2352

Defendant's Reply to Government Opposition (May 19, 2021) (Dkt. 354) SJA2360

Exhibit 1: Later Produced Screenshots of Target Website (Dkt. 354-1) SJA2368

Transcript of Proceedings held on May 7, 2021 (May 20, 2021) (Dkt. 355) (Pages 1-60) SJA2373

VOLUME 6

FILED UNDER SEAL

Continued from previous volume:

Transcript of Proceedings held on May 7, 2021 (May 20, 2021) (Dkt. 355) (Pages 61-85) SJA2433

Order (May 20, 2021) (Dkt. 363) SJA2459

Order (May 20, 2021) (Dkt. 364) SJA2466

Order (June 14, 2021) (Dkt. 402) SJA2475

Defendant's Memorandum on Admissibility of Rule 12.2(b) Evidence (June 21, 2021) (Dkt. 413) SJA2483

Order (June 23, 2021) (Dkt. 418) SJA2503

Defendant's Memorandum in Support of Motion to Supplement the Record and Renew His Motion to Compel Exculpatory Material or, in the Alternative, to Submit Exculpatory Material for *in Camera* Review (August 6, 2021) (Dkt. 427) SJA2507

Exhibit 1: 03/15/21 Discovery Letter (Dkt. 427-1) SJA2527

Exhibit 2: 03/15/21 Email (Dkt. 427-2) SJA2535

Exhibit 3: 04/21/21 Discovery Letter (Dkt. 427-3) SJA2537

Exhibit 4: 04/21/21 Email (Dkt. 427-4) SJA2540

Exhibit 5: Second Declaration of Anthony J. Ferrante (Dkt. 427-5) SJA2542

Reply to the Government's Opposition to Mr. Sanders's Motion to Supplement the Record and Renew His Motion to Compel Exculpatory Material or, in the Alternative, to Submit Exculpatory Material for *In Camera* Review (August 23, 2021) (Dkt. 443) SJA2559

United States' Response in Opposition to Defendant's Memorandum on Admissibility of Evidence Regarding a Mental Condition (September 3, 2021) (Dkt. 459) SJA2576

Memorandum in Support of Mr. Zackary Ellis Sanders's Renewed Motion to Suppress Based on Lack of Probable Cause and False and Misleading Statements and for a *Franks* Hearing (September 17, 2021) (Dkt. 467) SJA2607

Exhibit 2: Declaration of Professor Steven Murdoch (Dkt. 467-1) SJA2639

Order (September 21, 2021) (Dkt. 468) SJA2664

Memorandum in Support of Renewed Motion to Suppress Based on Warrantless Use of a Network Investigative Technique and False Material Information in Affidavit Paragraph 25 (September 24, 2021) (Dkt. 476) SJA2667

Zackary Sanders's Rule 16(b)(1)(C) Notice Regarding Dr. Fred S. Berlin (October 4, 2021) (Dkt. 481) SJA2699

Memorandum Opinion (October 12, 2021) (Dkt. 492) SJA2705

United States' Motion *in Limine* to Exclude the Testimony of Dr. Frederick S. Berlin (October 13, 2021) (Dkt. 498) SJA2730

Defendant's Opposition to the Government's Motion *in Limine* to Exclude the Testimony of Dr. Frederick S. Berlin (October 14, 2021) (Dkt. 511) SJA2730

Order (October 15, 2021) (Dkt. 512) SJA2745

Order (October 22, 2021) (Dkt. 525) SJA2749

Order (October 25, 2021) (Dkt. 533) SJA2757

Transcript of Trial Day 2 (October 20, 2021)[2] (Dkt. 556) SJA2762

VOLUME 7

FILED UNDER SEAL

Transcript of Trial Day 3 (October 21, 2021) (Dkt. 557) SJA2967

[2] The captions of the trial transcripts incorrectly show the trial dates as having occurred in November 2021.

Transcript of Trial Day 4 (October 22, 2021) (Dkt. 558) SJA3203

Transcript of Trial Day 5 (October 25, 2021) (Dkt. 559) (Pages 1-94) SJA3408

VOLUME 8

FILED UNDER SEAL

Continued from previous volume:

Transcript of Trial Day 5 (October 25, 2021) (Dkt. 559) (Pages 95-210) SJA3502

Transcript of Trial Day 6 (October 26, 2021) (Dkt. 560) SJA3618

Memorandum in Support of Motion for New Trial and to Reconsider Motions to Compel and Motions to Suppress (March 14, 2022) (Dkt. 588) SJA3845

Exhibit 1: Transcript of Motion Hearing, *United States v. Kiejzo*, No. 20-cr-40036-TSH (D. Mass. Sept. 17, 2021) (Dkt. 588-1) SJA3875

Exhibit 5: Complaint, *United States v. Zachary M. Stauffer*, No. 4:20-mj-04005-RJD (S.D. Ill. Jan. 28, 2020) (Dkt. 588-2) SJA3925

Exhibit 8: 03/04/2022 Government Email (Dkt. 588-3) SJA3935

Exhibit 20: Case Comparison Chart (Dkt. 588-4) SJA3940

Exhibit 44: FBI Operational Plan for Execution of Search Warrant (Dkt. 588-5) SJA3949

Notice of Filing of Two Supplemental Exhibits (March 17, 2022) (Dkt. 592) SJA3964

Exhibit 1: 3/23/2018 Report to Crown Counsel, *Regina v. Tyler David Walker* (Dkt. 592-1) SJA3970

Reply to the Government's Response to Motion for New Trial and to Reconsider Motions to Compel and Motions to Suppress (Dkt. 600) SJA4004

Memorandum Opinion (March 31, 2022) (Dkt. 615) SJA4026

Exhibit 9

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Property of [redacted], Pleasant

Case No. 1:20mj243

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and g*
the property located at [redacted], Pleasant Garden, NC, more particularly described in Attachment A of the affidavit.
located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence, fruits, and instrumentalities of violations 18 U.S.C. 2252, 2252A(a)(5)(B) and (b)(2), more specifically described in Attachment B of the affidvait.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(4)(B)	Possession with intent to view child pornography
18 U.S.C. § 2252A(a)(5)(B) and (b)(2)	Possession with intent to view child pornography

The application is based on these facts:
See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Brian Dexter
Applicant's signature

Brian Dexter, Special Agent
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: August 18, 2020

Judge's signature

City and state: Greensboro, North Carolina

L. Patrick Auld, U. S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Brian Dexter, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), since 2011, and am currently assigned to the HSI Winston-Salem office. While employed by HSI, I have investigated federal criminal violations related to child exploitation, and child pornography. I have gained experience through training at HSI and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I was previously employed as a United States Postal Inspector for approximately nine years. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at [redacted], Pleasant Garden, NC 27313 (the "SUBJECT PREMISES") and the content of electronic storage devices located therein, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § § 2252, 2252A(a)(5)(B) and (b)(2) which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of physical conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known

to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252, 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor

engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images,

or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

g. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

h. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications

devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. The "Domain Name System" or "DNS" is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

k. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

l. A "hidden service," also known as an "onion service," is website or other web service that is accessible only to users operating within the Tor anonymity network.

m. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

p. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

q. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

r. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

s. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

t. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

u. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

v. The "Tor network" is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit."

w. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

x. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

y. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and

receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein as the "TARGET WEBSITE."[1] There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE, as further described herein.

The Tor Network

7. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

[1] The name of the TARGET WEBSITE is known to law enforcement. Investigation into the users of the website remains ongoing and disclosure of the name of the website would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

8. The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

9. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.[2] The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

10. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily

[2] Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

(and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

11. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

12. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the

Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

13. The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

14. Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example "asdlk8fs9dflku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly

available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

Description of TARGET WEBSITE 1

15. The "TARGET WEBSITE 1" was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children that operated from approximately October 2016 to June 2019. In June of 2019, the computer server hosting the TARGET WEBSITE 1, which

was located outside of the United States, was seized by a foreign law enforcement agency.

16. While it operated, the website administrator posted a message on the website describing its purpose as being to "share cp of babies and toddlers." The term "cp" in this context refers to child pornography. The name of the TARGET WEBSITE 1 contained a reference to children of that age and the website logo included images depicting babies and toddlers. The TARGET WEBSITE 1 name itself is a reference to the genitalia of prepubescent boys. The TARGET WEBSITE 1 allowed users to make and view postings that contained text, still images, video images, and/or web links that directed members to specific content located on another website. The TARGET WEBSITE 1 also had a private message feature that allowed users to send private messages to each other.

17. The TARGET WEBSITE 1 also had a separate, selective membership section that provided such members with exclusive child pornographic content. To join that selective membership, members were required to upload nude or sexually explicit images depicting babies and toddlers. As of June 2019, the website had over 230,000 members and over 29,000 postings. While it operated, HSI Special Agents accessed the

TARGET WEBSITE 1 and downloaded digital child pornography content accessible via the website, in an undercover capacity.

18. Upon accessing the TARGET WEBSITE 1, the initial web page revealed a message board including links a user would access to register and log-in, as well as hyperlinked message board headings titled, "Announcements," "Rules," "Allowed Hosts," "How to post," "Security," and "Apply for VIP." Upon accessing the "Apply for VIP" hyperlink on the TARGET WEBSITE 1, users would observe the following text:

> Forum Rules, Application for VIP:
>
> - Only child porn (nude or sex) pics or videos of babies and toddler
>
> - All archives must be encrypted in Rar or 7Zip format
>
> - The archive passwords must contain your nickname and [TARGET WEBSITE 1 name]
>
> - Don't forget provide a live preview
>
> - Only use safe hosts without javascript
>
> - No need to apply with private stuff. Random CP of 0-5yo is accepted (boys and girls).

19. Based upon my training an experience, I am aware that "Rar" and "7Zip" refer to archive files, which are a method of storing multiple

digital files (image or videos for example) in a single, compressed file, which may be password-protected; that a "live preview" consists of a representative sub-set of a set of still images or still shots from a video, which give a user a preview of the full image set or video available for download; and a "safe host" refers to a file hosting provider on whose servers password-protected digital files may be stored, which is perceived by users of the website to not be compliant with law enforcement requests for information.

20. Upon accessing the "Register" link of the TARGET WEBSITE 1, users completed a "Username," and "Password," field, as well as a "Confirmation" code to enter the website. Located at the bottom of the web page are two additional sections entitled "The Team" and "Delete All board cookies." "The Team" section listed the usernames of three website "Administrators."

21. After successfully registering, a user was taken to a web page stating that an account has been created and the user may login with username and password. A user was then able to access the "Board Index." Sections for posting to the website within the Board Index included: "CP Stars," with forums "Boys" and "Girls;" "Babies (0-1YO)," with forums "Baby

Boys" and "Baby Girls;" and "Toddlers (2-5YO)," with forums "Toddler Boys" and "Toddler Girls."

22. Upon accessing a user posting on the website, the original post appeared at the top of the page, with any corresponding replies to the original post included in the thread below it. Typical posts contained text, images, links to external sites, or replies to previous posts. A review of postings within these sections revealed numerous posts containing images depicting child pornography and child erotica of prepubescent males, females, toddlers, and infants. Examples of these are as follows:

23. On May 14, 2017, a website administrator posted a topic entitled "We are back" in the "Announcements" forum that contained the following statement: "Only CP contributors will have access now to the stuff. If you are not VIP, make your application for member..." The post contained an image depicting a prepubescent male, who appeared naked below the waist exposing his genitals, and featured a green post it note reading, "May-13-2017" along with what appeared to be the username of another website administrator. Among other things, the image focused on the exposed penis of the prepubescent male. Based upon my training and experience, the significance

of this posting was to effectively make membership available only to those users who uploaded child pornography to the website.

24. On May 23, 2017, a website administrator posted a message entitled "Inactive" in the "Announcements" forum that contained the following: "Abandoned accounts was automated deactivated. VIP accounts will be also automated deactivated after 2 months, if they not make any contribution." Based on my training and experience, a "contribution" means a posting to the website, generally one that contains or provides a link to child pornography images/videos. Below the text of the post, a photo of a prepubescent female child with her legs spread, focusing on her vagina, was displayed. In the top left of the photo were textual graphics that included what appeared to be usernames of website users and administrators as well as the term "1yo," and a torn green post-it note that read, "[TARGET WEBSITE 1 name]," contained the web address for TARGET WEBSITE 1, and the text "Exclusive 0-5yo NEW 2017."

25. On June 30, 2017, a review of the website revealed a post from a website member titled "Toddler Fuck" in the "Toddlers (2-5yo)" forum. The post contained an image depicting a prepubescent male toddler, appearing naked and exposing his genitals, on his back while an adult male penis

entered his anus. The image focused on the exposed adult male penis penetrating the toddler.

26. In addition, postings to the TARGET WEBSITE 1 that were publicly available to any registered user of the TARGET WEBSITE 1 were captured and archived for law enforcement review. Review of such postings disclosed the following posts by TARGET WEBSITE 1 users.

27. Your affiant reviewed five (5) images that depicted sexually explicit images of minors that were made available on the TARGET WEBSITE 1. Below are descriptions of the five (5) images;

a. This is a color image comprised of video frame captures of a naked 8 to 10-year-old female lying on her back with her legs spread. An adult male's erect penis is being inserted into the child's anus.

b. This is a color image comprised of video frame captures of a naked 2 to 4-year-old female who is lying on her side and back. The image is zoomed-in on the child's genitalia while an adult male's finger and erect penis are inserted into the child's vagina and anus.

c. This is a color gif image of a partially naked 3 to 5-year-old female who is lying on her side while an adult male's erect penis is inserted into the child's anus.

d. This is a color gif image of a partially naked 2 to 4-year-old female lying on her back while an adult male is inserting his erect penis into the child's anus.

e. This is a color image of a naked newborn, under the age of 1 to 2 weeks old, male who is lying on his back in a hospital basinet. The infant's legs are spread apart and the child's genitals are exposed and visible.

Description of TARGET WEBSITE 2

28. The TARGET WEBSITE 2 was an online bulletin board dedicated to the advertisement and distribution of child pornography that operated from approximately at least September 2016 to June 2019. In June of 2019, the computer server hosting the TARGET WEBSITE 2, which was located outside of the United States, was seized by a foreign law enforcement agency.

29. A review of the initial TARGET WEBSITE 2 page revealed it was a message board web page that contained a search bar, and showcased two hyperlinks titled, "Announcements" and "Important Information." Located below the title were hyperlinks including those entitled "Quick Links," "Home," "Board Index," "Login," and "Register." As of June 2019, the website had over 820,000 members and over 81,000 postings.

30. Upon accessing the "Announcements" hyperlink of the TARGET WEBSITE 2, the following message was displayed in message board form, "Welcome, Please read before registering" which was dated July 1, 2016. Upon accessing the aforementioned hyperlink, the message read, "Welcome

abusers and abusees and those that enjoy watching. This website was created to host videos, photos and discussions of 18 (twinks) and younger of Hurtcore materials (videos & pictures) as well as discussion of such." Based on my training and experience, I know that Hurtcore refers to violent pornography. The message continued, "PS Please register to see all the forums, and use strong password for user profile."

31. Upon accessing the "Register" link of the TARGET WEBSITE 2, it was revealed that users would complete a "Username," "Password," "Confirm password," "Language," and "My timezone," fields, as well as a "Confirmation of Registration" code. Upon entering the TARGET WEBSITE, sections and forums for posting to the website included "HURTCORE Toddlers Videos (Ages 0-5)," "Preteen/Hebe Children Videos (Ages 6-13)," "Teens Videos (Ages 14+)," "Toddlers Images (Ages 0-5)," "Preteen/Hebe Children Images (Ages 6-13)," and "Teens Images (Ages 14+)." Based on my training and experience, I know that "Hebe" is a reference to a ("hebephile," which is a person with a persistent sexual interest in pubescent minor children. Another forum was named "GORE/DEATH" which included sub-forms for "Toddlers (Ages 0-5)," "Preteen/Hebe Children (Ages 6-13)" and "Teens (Ages 14+)." An additional section of the website called "The Team"

listed the usernames of two website "Administrators" and five "Global Moderators." The TARGET WEBSITE 2 also contained a private message feature that was available, allowing users to send private messages to each other.

32. On June 23, 2016, a website administrator posted a topic entitled "Board Rules" in the "Important Information" forum which contained the following explanation of the website:

Rules are simple all material must be related to Hurtcore content. What is Hurtcore content? It is rape, fighting, wrestling, bondage, spanking, pain, mutilation, gore, dead bodies, and etc. (no limits) Why does this place exist? There was a need and since society thinks I am worst than any abuser or creator of Hurtcore content, I decided to create this place for those who like it and want to share. Besides I am the mischievous god. It is up to you to make this the best Hurtcore board there is. So please upload whatever you can so that it can be shared.

33. A review of the "Toddlers Videos," "Preteen/Hebe Children," "Toddlers Images," and "Gore/Death" forums and subforums, as well as additional forums, within the various above sections revealed they contained numerous pages of topics. Each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the thread below it.

Typical posts appeared to contain text, images, thumbnail previews of images, links to external sites with compressed files (such as ".rar"), or replies to previous posts.

34. A review of topics within these sections revealed numerous posts containing images and/or videos depicting child pornography and child erotica of prepubescent males, females, toddlers, and infants; including those depicting anal, vaginal, and oral penetration. Additionally, these sections revealed numerous posts containing images and/or videos depicting child pornography involving gore and sometimes death. Examples of these are as follows:

35. On October 9, 2016, a website user posted a topic entitled "Fuck the newborn. Real fuck!" in the "Hurtcore/Toddlers Images/Girls" forum, that contained nine images depicting child pornography and child erotica of a prepubescent female infant. One of these images depicted a naked female infant lying on her back with her legs spread apart, exposing her vagina, with a gloved adult finger inserted into her anus. A male's penis was pressed against her vagina and the head of the penis inserted into her mouth. A brown liquid substance, appearing to be the infant's feces are seen smeared around her anus.

36. On November 5, 2016, a website user posted a topic entitled "BabyHee 1yo (one of full version)" in the "HurtCore/Toddlers Videos/Boys" forum that contained images depicting child pornography and torture of a prepubescent male, who was completely naked and tied down with rope on the side of a bath tub. Among other things, the images depicted an adult male defecating on the chest and urinating in the mouth of the prepubescent male.

37. In addition, postings to the TARGET WEBSITE 2 that were publicly available to any registered user of the TARGET WEBSITE 2 were captured and archived for law enforcement review. Review of such postings disclosed the following posts by TARGET WEBSITE 2 users:

38. Your affiant reviewed five images that depicted sexually explicit images of minors that were made available on the TARGET WEBSITE 2. Below are descriptions of the five (5) images:

a. This is a color image comprised of video frame captures of a naked 4 to 6-year-old female, zoomed in on the child's genitalia. An adult's hands are spreading the child's genitalia apart in order to see the inside of the child's vagina.

b. This is a color image comprised of video frame captures of a naked 3 to five-year-old female who is sitting on a toilet and urinating. The image zooms in on the child's genitalia while she is urinating.

c. This is a color image comprised of video frame captures of a naked 4 to 6-year-old female who is on her hands and knees on a

bed. An adult's hand is seen inserting a sex toy and an erect penis into the child's anus, prior to displaying the child urinating into a glass jar.

d. This is a color video of a naked 2 to 4-year-old female laying on her side on a bed. An adult's hand is seen inserting a finger and an erect penis into the child's vagina. The child appears unresponsive.

e. This is a color image comprised of video frame captures of a naked 3 to 5-year-old female laying on her back on a bed. An adult male is seen performing oral sex on the child. The frame captures then changes to showing the same female sitting on a toilet defecating while an adult male's penis is held near the child as if masturbating.

Description of TARGET WEBSITE 5

39. The TARGET WEBSITE 5 was an online chat site whose primary purpose is to share and distribute child pornography. The advertisement and distribution of child pornography and child erotica were regular occurrences on this site. The TARGET WEBSITE 5 started operating in approximately 2018 and appeared to cease operating in 2020.

40. On the front page of the site, it stated that the site was intended for users to "post links with good photos and videos" depicting "[o]nly GIRLS 4 to 14 years [old]." The site allowed users to engage in online chat with other users, either within chat rooms that were openly accessible to any user of the site, within rooms only accessible to particular users, or in

one-to-one chats between two users. Child pornography images and videos were trafficked through this chat site via the posting of web links within chat messages. Links allowed a user to navigate to another website, such as a file-hosting website, where images and/or videos were stored in order to download these image and videos. The TARGET WEBSITE 5 provided its users with information about particular file hosting websites where users could upload digital files so that the files could then be shared, via links, with other users on the TARGET WEBSITE 5.

41. Entry to the site is obtained through free registration, as described below. On the registration page, it reads, among other things, "No hurtcore, No gore, No zoo, No death, No toddlers." In my training and experience, "zoo" refers to pornography depicting bestiality, and "hurtcore" is a genre of child pornography that depicts violence, gore, torture, humiliation, or children in pain and distress. In addition, the registration page of the TARGET WEBSITE 5 expressly contemplated the sharing of videos between members. Language on that page reads "Post links with good photos and videos (preview is required!)."

42. In order to pass through the registration page and gain access to the actual content of the TARGET WEBSITE 5, a prospective user

must create a "Nickname" and a password which must be entered along with a Captcha. A "Captcha" is a randomly generated series of characters designed to ensure that users of a website are human beings and not bots or other automated processes. Users are not required to enter any personally identifiable information, such as true names, emails or phone numbers. The users may also pick a color for their posts (or one was randomly generated) and click "enter chat."

43. Upon initially creating a user account on the TARGET WEBSITE 5, a user was assigned the status of "Guest." As an unregistered user, the user receives the following message upon log in: "As it looks like you are not registered you may check our rules by sending to me word rules. There also will be some additional explanation of how to use this feature. News! We added feature of forum. Access by button at the bottom or just by this link: forum. this should make you be more happy of getting this message on entrance." Unregistered or "Guest" users could access TARGET WEBSITE 5 postings including postings that shared child pornography images.

44. In order to fully register an account, the user would need to obtain a promotion from "Guest" to "Registered Guest," which is done at the discretion of TARGET WEBSITE 5 staff. After an individual is promoted to a

registered user account on the TARGET WEBSITE 5, a user must log in to that user account with the appropriate user-generated password in order to communicate via that user account on the TARGET WEBSITE 5. TARGET WEBSITE 5 users may register, log into and access the TARGET WEBSITE 5 through that user account using any computer or electronic device that is configured to use Tor routing/software.

45. As is common on these types of sites, the TARGET WEBSITE 5 was administered and moderated by select TARGET WEBSITE 5 users referred to as "Members" on this site. These users are promoted at the discretion of the site leadership. Promotions appeared to be made based on an individual's active participation on the site. Once promoted to a Member position, those users enforced the rules and assisted in the management of the site. This included controlling user membership using the "ban" and "kick" functions (which can limit or eliminate a user's participation or account), promoting within the ranks of users, and moderating the public chatroom for content and user behavior.

46. TARGET WEBSITE 5 Members periodically re-posted standard messages to the public chatroom of the TARGET WEBSITE 5 iterating rules and procedures of the TARGET WEBSITE 5. For example, on or about May

28, 2019, a Member on the TARGET WEBSITE 5 posted "CHAT RULES" in the public chatroom. This post contained statements in both Russian and English which included but was not limited to, "Follow the requests of the Members," "No hurtcore, No gore, No zoo, No death, No toddler," "Only GIRLS 5 to 13 years. Any language allowed," and "For RG (registered guests) the photo archive is available (the "links" button)."

47. Also on or about May 28, 2019, a Member posted "SECURITY INFORMATION" in the public chatroom. This post contained statements in both Russian and English which included but was not limited to the following:

- Set the Security Slider to HIGH Security Level
- Do Not Download if you are not using Encryption or Tails OS
- Read these manuals: □ Tails Guide & Tor Security Guide □

Do Not Share any Identifying Information & NEVER Trust Anybody!

Windows & OS X/MacOS are not safe for On topic

Save files only to Encrypted Storage

Windows Leaves traces you cannot clean without a Full disk wipe

Linux offers Full Disk Encryption, Tails is Amnesic

use VeraCrypt to create Hidden Encrypted Containers

Open files when Offline to lower risk of malicious file causing trouble

LEA & Antis are known to pose as parents and kids to trick you into revealing information to them, suspect everyone is LEA.

LEA could be running this or any site at any time

Always be conscious your messages may not be private

Be Careful Paying for Anything, Bitcoin is not Anonymous by default!

When a user posts in the open chat, other users can see the name of the poster, what was posted and what time it was posted. Images posted to the site can be categorized or "tagged" by users based upon the image theme or characteristics. These tags aid users in searching for specific types of content.

48. There was also an advertisement in the middle of the TARGET WEBSITE 5 chat screen stating, "VISIT OUR SITES" and it features four links to other Tor sites. Each site has a short description along with a link to the Tor web address for the site. The descriptions state: "Forum for boy-and girlovers" with a link to another website; "Chat for boylovers" – with a link to another website; "Girls pedo portal", and "only Ru". Based on my training and experience, I am aware that the reference to "only Ru" means that site is

only for Russian speakers. Further, based on my training and experience, it is apparent that these websites are associated with each other.

49. The TARGET WEBSITE 5 provided users with numerous links to image hosts where users can upload their digital images. For instance, on November 2, 2018, a TARGET WEBSITE 5 user posted a hyperlink of a .jpeg file that linked to an image of a prepubescent girl having her underwear pulled down and a male penis resting on her inner thigh near her exposed vagina. In another instance, on March 1, 2019, a TARGET WEBSITE 5 user posted a hyperlink of a .jpg file that linked to an image of a prepubescent female bent forward on what appears to be a wooden chair with her back towards the camera. She was wearing a black and red skirt and no underwear. The female's anus and vagina are prominently exposed for the camera. Her face was turned to the side making it partially visible through her hair. The female had no pubic hair, was small in stature, and young facial features. Also, on May 27, 2019, a TARGET WEBSITE 5 user posted a hyperlink to a .jpg image depicting a nude prepubescent female laying on a bed. The image only showed the male's torso and upper leg from the side. The adult male was pushing his erect penis into the female's mouth.

50. Postings to the TARGET WEBSITE 5 that were publicly available to any registered user at the time of posting were captured and archived for law enforcement review. Over 1,200,000 messages were posted on the TARGET WEBSITE 5 between March 2018 and March 2020 when the site appeared to go offline. FBI Special Agents have accessed and downloaded child pornography files via links that were posted on TARGET WEBSITE 5, in an undercover capacity.

51. FLA described the website as facilitating "the sharing of child sexual abuse and exploitation material, stipulating only girls aged 5 – 13. Users were required to enter a username and password but these were only valid for that single login session" and provided further documentation naming the website as the TARGET WEBSITE 5, which the FLA referred to by its actual name.

52. Your affiant reviewed five images that depicted sexually explicit images of minors that were made available on the TARGET WEBSITE 5. Below are descriptions of the five (5) images:

a. This is a color image of a naked 8 to 10-year-old female and a naked adult male. The child is being bent over a table while the adult is having sex with her.

b. This is a color image of three naked children and a naked adult male. The children appear to be 1 to 3 years of age, 4 to 6 years

of age, and 10 to 12 years of age, respectively. The adult male is lying on his back on a bed while the 4 to 6-year-old female is straddling him and holding his erect penis near her genitalia. The 1 to 3-year-old female is lying on her back beside the adult's head. The 10 to 12-year-old female is seen closest to the camera as if taking a "selfie" (self-portrait style) photo.

c. This is a color image of four naked female children on a bed. One child is 1 to 3 years of age and is sitting on the bed. One child is 10 to 12 years of age and is laying on her stomach. One child is 5 to 8 years of age and is standing on the bed. The last child is 8 to 10 years of age and is also standing on the bed.

d. This is a color image of a naked 5 to 7-year-old female lying on her back. An adult male is standing above her while she is holding his erect penis in both hands.

e. This is a color image of a naked 5 to 7-year-old female with a naked adult male standing behind her and holding her legs. The end of the adult's penis can be seen between the child's legs and pressed against her genitalia.

Evidence Related to Identification of Target that Accessed TARGET WEBSITES

53. I am aware that U.S. as well as foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the website(s) described herein. Those websites are globally accessible. The websites and their users may therefore be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the

beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the website is located or the offender appears to reside, in accordance with each country's laws.

54. In August 2019, a foreign law enforcement agency (referenced herein as "FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that FLA determined that on April 22, 2019 through May 17, 2019, three (3) different dynamic IP addresses (**74.177.187.154**; **74.177.187.134**; **74.177.188.208**) were used to access online child sexual abuse and exploitation material via the three websites that the FLA named and described as TARGET WEBSITES 1, 2, and 5.

TARGET WEBSITE LEADS

55. FLA described the target websites as having "an explicit focus on the facilitation of sharing child abuse material (images, links and videos)," stated that "[u]sers were required to create an account (username and password) in order to access the majority of the site[s] and hosted material,"

and provided further documentation naming the sites as TARGET WEBSITES 1, 2, and 5, which the FLA referred to by its actual name.

56. FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

57. I am aware through my training and experience and consultation with other U.S. law enforcement agents that tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites have: (1) led to the identification

and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

58. As described herein, the TARGET WEBSITES could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software on the user's computer could access the TARGET WEBSITES. Even after connecting to the Tor network, however, a user would have to find the 16-or-56-character web address of the TARGET WEBSITES in order to access them. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography

websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory website in order to access it. While it operated, the web address for the website described herein was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

59. I am also aware through consultation with FBI agents that the review of detailed user data related to one Tor network-based child pornography website found that it was exceedingly rare for a registered website user to access that website and never return. FBI review of user data from that website found that less than two hundredths of one percent of

user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the website and logged in to the same account.

60. Accordingly, based on my training and experience and the information articulated herein, because accessing the TARGET WEBSITES required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITES, and then connecting to TARGET WEBSITES via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITES without understanding their purpose and content.

61. Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed the TARGET WEBSITES has, at a minimum, knowingly accessed the TARGET WEBSITES with intent to view child pornography or attempted to do so.

Identification of SUBJECT PREMISES

62. HSI Boston Special Agents received information, from a foreign law enforcement partner, that on May 07, 2019 at 23:53:31 UTC an individual originating from IP address **74.177.187.154** accessed a known darkweb site that facilitated the sharing of child sexual abuse and

exploitation material. This darkweb site contained child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on babies and toddlers (ages 0-5 years old). Users were required to create an account (username and password) in order to access the majority of the site and hosted material.

63. According to the publicly available information, IP address **74.177.187.154**– the one used to access **TARGET WEBSITE 1**, as described above – is owned/operated by AT&T. On or about November 22, 2019 a summons (568566) was served on AT&T for the subscriber assigned IP address: **74.177.187.154** on May 07, 2019 at 23:53:31 UTC. AT&T provided their response with the following subscriber details:

Subscriber Name: Anita Mastriaco
Service Address: [redacted]**, Pleasant Garden, NC 27313**
Additional Address Details: (TK 220 Exit 62 Tk Lft 6-8 ML to Lght Tk Rght Racine 1ML)
DSL Phone: 336-685-5964
Email Address: anthonyanita@bellsouth.net
Account Status: Open
Usage Start: 05/04/2019 12:27 AM
Usage End: 05/13/2019 11:19 AM

64. HSI Boston Agents received information, from a foreign law enforcement partner, that on April 22, 2019 at 01:58:13 UTC an individual originating from IP address **74.177.187.134** and May 17, 2019 at 01:31:15 UTC an individual originating from the IP address: **74.177.188.208** accessed a known darkweb site that facilitated the sharing of child sexual abuse and exploitation material. This darkweb site contained child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children. Users were required to create an account (username and password) in order to access the majority of the material.

65. According the publicly available information, IP addresses **74.177.187.134** and **74.177.188.208** – the ones used to access **TARGET WEBSITE 2**, as described above – are owned/operated by AT&T. On or about December 3, 2019 a summons (570024) was served on AT&T for the subscriber assigned IP addresses: **74.177.187.134** on April 22, 2019 at 01:58:13 UTC. AT&T provided their response with the following subscriber details:

Subscriber Name: **Anita Mastriaco**

Service Address: [redacted], **Pleasant Garden, NC 27313**
Additional Address Details: (TK 220 Exit 62 Tk Lft 6-8 ML to Lght Tk Rght Racine 1ML)
DSL Phone: 336-685-5964
Email Address: anthonyanita@bellsouth.net
Account Status: Open
Usage Start: 04/17/2019 07:42 PM
Usage End: 04/29/2019 08:17 PM

66. On or about December 3, 2019 a summons (570024) was served on AT&T for the subscriber assigned IP addresses: **74.177.188.208** on May 17, 2019 at 01:31:15 UTC. AT&T provided their response with the following subscriber details:

Subscriber Name: Anita Mastriaco
Service Address: [redacted], **Pleasant Garden, NC 27313**
Additional Address Details: (TK 220 Exit 62 Tk Lft 6-8 ML to Lght Tk Rght Racine 1ML)
DSL Phone: 336-685-5964
Email Address: anthonyanita@bellsouth.net
Account Status: Open
Usage Start: 05/13/2019 11:34 PM
Usage End: 05/18/2019 09:55 AM

67. HSI Boston Special Agents received information, from a foreign law enforcement partner, that on April 22, 2019 at 02:03:22 UTC an individual originating from IP address **74.177.187.134** and on May 07, 2019 at 23:29:36 UTC an individual originating from IP address **74.177.187.154**

accessed a known darkweb chat site whose primary purpose is to share and distribute child pornography. The advertisement and distribution of child pornography and child erotica are regular occurrences on this site. On the front page of the site, it states that the site is intended for users to "post links with good photos and videos" depicting "[o]nly GIRLS 5 to 13 years [old]."

68. According the publicly available information, IP addresses 74.177.187.134 and 74.177.187.154 – the ones used to access **TARGET WEBSITE 5**, as described above – are owned/operated by AT&T. On or about November 22, 2019 a summons (568621) was served on AT&T for the subscriber assigned IP address: **74.177.187.134** on April 22, 2019 at 02:03:22 UTC. AT&T provided their response with the following subscriber details:

Subscriber Name: Anita Mastriaco
Service Address: [redacted], Pleasant Garden, NC 27313
Additional Address Details: (TK 220 Exit 62 Tk Lft 6-8 ML to Lght Tk Rght Racine 1ML)
DSL Phone: 336-685-5964
Email Address: anthonyanita@bellsouth.net
Usage Start: 04/17/2019 07:42 PM
Usage End: 04/29/2019 08:17 PM

69. On or about November 22, 2019 a summons (568621) was served on AT&T for the subscriber assigned IP address: **74.177.187.154** on May 07,

2019 at 23:29:36 UTC. AT&T provided their response with the following subscriber details:

Subscriber Name: Anita Mastriaco
Service Address: [redacted], Pleasant Garden, NC 27313
Additional Address Details: (TK 220 Exit 62 Tk Lft 6-8 ML to Lght Tk Rght Racine 1ML)
DSL Phone: 336-685-5964
Email Address: anthonyanita@bellsouth.net
Usage Start: 05/04/2019 12:27 AM
Usage End: 05/13/2019 11:19 AM

70. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for Anita MASTRIACO. These public records indicated that Anita MASTRIACO's current address is [redacted], Pleasant Garden, NC 27313 (SUBJECT PREMISES). In addition, these public records indicated that Anita MASTRIACO's partner, Alice SIEG, and son, Nicholas MASTRIACO, also reside at the SUBJECT PREMISES.

71. A check with the North Carolina Department of Motor Vehicles on or about August 5, 2020 revealed that an individual named Anita M. MASTRIACO with a date of birth of [redacted], 1962 resides at the SUBJECT PREMISES.

72. A check with the North Carolina Department of Motor Vehicles on or about August 5, 2020 revealed that an individual by the name of Nicholas J. MASTRIACO with a date of birth of [redacted], 2000 resides at the SUBJECT PREMISES.

73. On or about July 7, 2020, representatives of the U.S. Postal Service stated that individuals with the last name MASTRIACO are currently receiving mail at the SUBJECT PREMISES.

74. On or about August 5, 2020, your affiant observed the residence at the SUBJECT PREMISES. The driveway from [redacted] up to the residence has a dark red/maroon in color "cattle gate" (fence) preventing anyone, or any vehicles from entering on to the property of the SUBJECT PREMISES. The residence is a single-story family residence with dark red/maroon in color vinyl siding, a white in color two-car garage door, white in color trim around the outer portions of the residence and windows, and black in color shutters outside of the windows. There is also an American flag hanging by a pole affixed above the garage door. Your affiant observed a dark grey/charcoal in color Dodge pick-up truck bearing North Carolina registration HAS-1122 parked in the driveway in front of the garage door.

According to North Carolina DMV records, the vehicle is registered to Anita M. MASTRIACO.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

75. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera

or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that

photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also

referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web

cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

76. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to

lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted

child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[3]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of

[3] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

77. Based on all of the information contained herein, I believe that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access online child sexual abuse and exploitation material via a website. In particular, the target of investigation obtained and used Tor network software, found the web address for TARGET WEBSITE, and accessed online child sexual abuse and exploitation material via the TARGET WEBSITE.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

78. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records

are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

79. I submit that if a computer, smartphone, or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later

using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

80. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct

evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in

which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or

used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a

computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer

behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct

was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

81. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel

who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions.

For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

82. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to

connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

83. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of

the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

84. This warrant permits law enforcement to compel Joseph LAWSON to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID,"

which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted

Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Anita MASTRIACO, Alice SIEG, or Nicholas MASTRIACO to the fingerprint scanner of the DEVICES found at the SUBJECT PREMISES; (2) hold the DEVICES found at the SUBJECT PREMISES in front of the face of Anita MASTRIACO, Alice SIEG, or Nicholas MASTRIACO and activate the facial recognition feature; and/or (3) hold the DEVICES found at the SUBJECT PREMISES in front of the face of Anita MASTRIACO, Alice SIEG, or Nicholas MASTRIACO and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed

warrant does not authorize law enforcement to compel that Anita MASTRIACO, Alice SIEG, or Nicholas MASTRIACO state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel Anita MASTRIACO, Alice SIEG, or Nicholas MASTRIACO to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

85. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A and authorizing the seizure and search of the items described in Attachment B.

86. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later

be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

/s/ Brian E. Dexter

/s/Brian E. Dexter
Special Agent
Homeland Security Investigations

On this 18th day of August 2020, Brian E. Dexter appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Affidavit.

L. PATRICK AULD
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The entire property located at [redacted], Pleasant Garden, NC 27313, the residence is a single-story family residence with dark red/maroon in color vinyl siding, a white in color two-car garage door, white in color trim around the outer portions of the residence and windows, and black in color shutters outside of the windows. There is an American flag hanging by a pole affixed above the garage door. There is a black in color mailbox at the bottom of the driveway. The vertical post of the mailbox prominently displays [redacted] with black in color stensil with silver backdrop. There is also a metal sign hanging underneath the mailbox with the following: "Fresh Eggs For Sale $3.00 A Dozen". There is a dark red/maroon in color gate across the driveway of the residence. A "POSTED – Private Property" sign, and a "BEWARE OF DOG" sign are affixed to the gate. See attached photographs.




POSTED
BEWARE
OF THE DOG

ATTACHMENT B

ITEMS TO BE SEARCHED AND/OR SEIZED

This warrant authorizes (i) the search of the property identified in Attachment A for only the following and (ii) authorizes the seizure of the items listed below only to the extent they constitute the following:

(a) evidence of violations of 18 U.S.C. §§ 2252 and 2252A ("subject violations"); or

(b) any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession is illegal due to the subject violations; or

(c) any property designed for use, intended for use, or used in committing any subject violations.

Subject to the foregoing, the items authorized to be seized are:

1. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created,

edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

h. records of or information about Internet Protocol addresses used by the COMPUTER;

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items reflecting the occupancy or ownership of the SUBJECT PREMISES, [redacted] Road, Pleasant Garden, NC 27313 including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items reflecting the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information reflecting the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or

optical media.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel Anita MASTRIACO, Alice SIEG, or Nicholas MASTRIACO to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the DEVICES found at the PREMISES, and

(b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES's security features in order to search the contents as authorized by this warrant, but only if Anite MASTRICAO, Alice SIEG, or Nicholas MASTRIACO are present at the PREMISES at the time of execution and the process is carried out with dispatch in the immediate vicinity of the PREMISES.

This warrant does not authorize law enforcement personnel to compel any other individuals not residing, but otherwise found at the PREMISES, to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to compel that individuals residing at the PREMISES state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

Exhibit 10

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Vermont

U.S. DISTRICT COURT
DISTRICT OF VERMONT
FILED

2020 DEC -4 PM 3:12

CLERK

BY LAW
DEPUTY CLERK

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

[redacted] Burlington, VT

Case No. 2:20-mj-143-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, incorporated herein.

located in the _____ District of Vermont, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2); 18 U.S.C. § 2252A(b)(1); 18 U.S.C. § 2252A(a)(5)(B); 18 U.S.C. § 2252A(b)(2)	Receipt of child pornography, possession of and access with intent to view child pornography, and attempt and conspiracy to commit those crimes.

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Seth Fiore, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/04/2020

Judge's signature

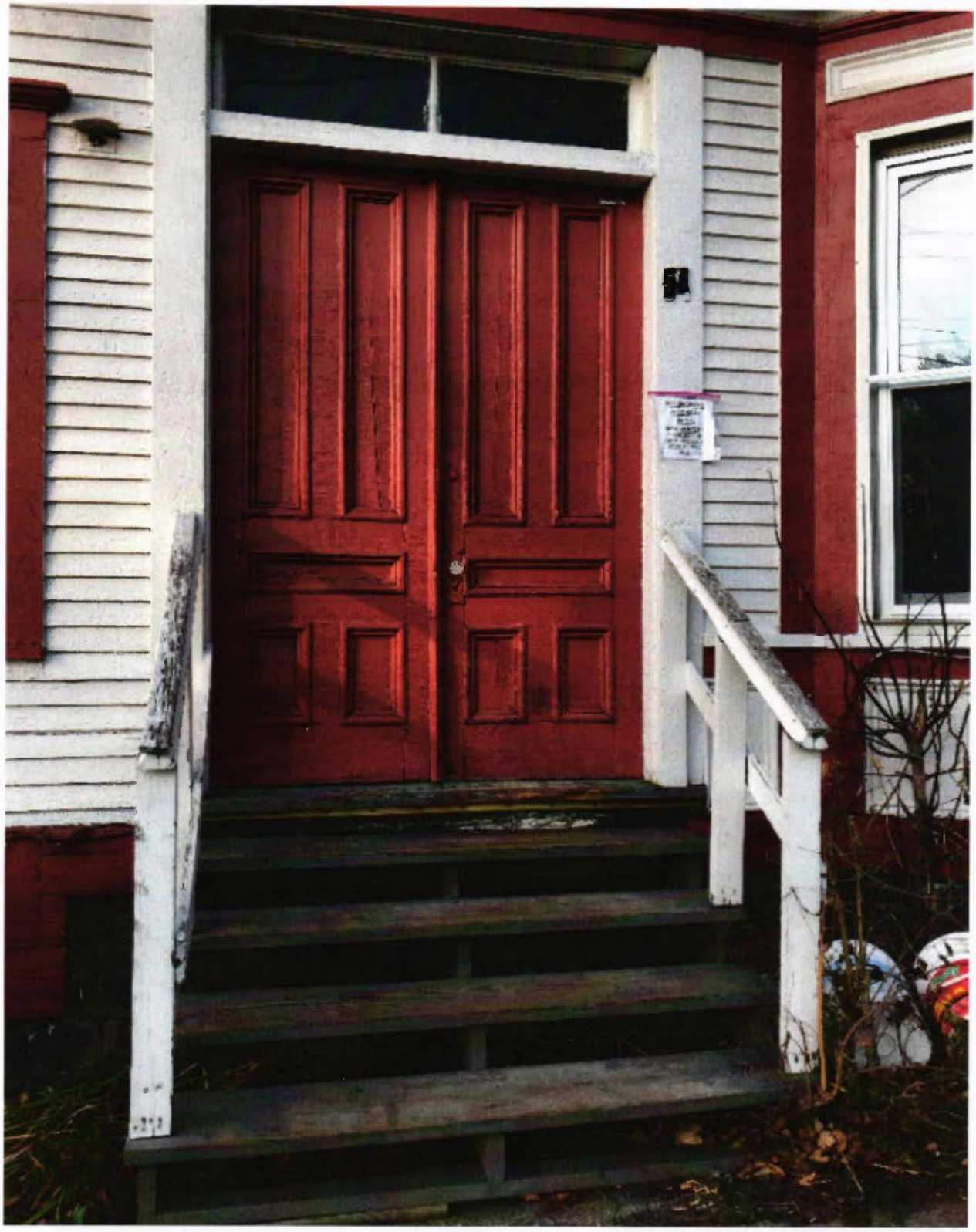
City and state: Burlington, VT

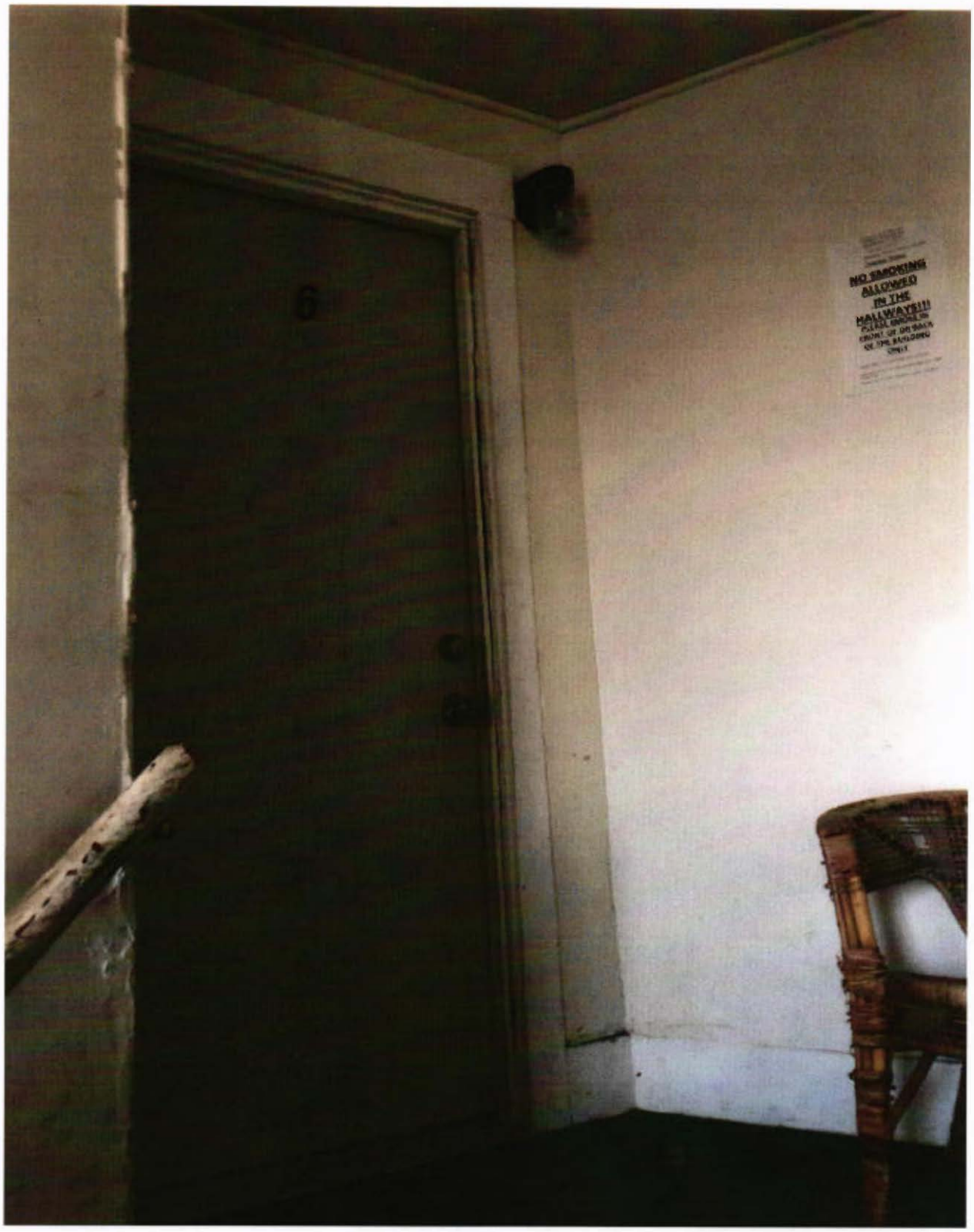
Hon. John M. Conroy, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

The property to be searched is [redacted] Burlington, Vermont, the TARGET PREMISES. The TARGET PREMISES is an apartment within a multi-level, multi-family dwelling. The building is painted white with red trim, with a main entryway on Spruce St. accessed by red doors. A black [redacted] over white is located aside from the red doors at the main entryway. Inside, apartments are identified by numbers affixed to or around doors. On the third floor, a black [redacted] is affixed to an apartment door.






NO SMOKING
ALLOWED
IN THE
HALLWAYS!!!

ATTACHMENT B

All property, records, and information, in any format, that constitute fruits, evidence and instrumentalities of violations of 18 United States Code §§ 2252A(a)(2) and (b)(1) (receipt of child pornography), and §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), and attempt and conspiracy to commit those crimes, ("the Target Offenses"), for the time period from April 12, 2019 to present (unless otherwise indicated), including, but not limited, to the following items:

1. Computers, cellular telephones and storage media, as defined below (hereinafter, "device(s)"), used as a means to commit the TARGET OFFENSES;

2. Child pornography, as defined in 18 U.S.C. § 2256(8), and/or visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

3. Any and all information, notes, documents, records, or correspondence, in any format or medium, pertaining to child pornography or sexual activity with or sexual interest in minors;

4. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the digital file(s), or that aid in the identification of persons involved in violations of the TARGET OFFENSES;

5. Records and information relating to the access, viewing or trafficking of child pornography, including correspondence and communications;

6. Records, information, and items relating to the occupancy or ownership of the TARGET PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

7. Records, information, and items relating to control and use of a Burlington Telecom internet subscription, including bills, mail envelopes, and payment information, including checking account, credit or debit card account information;

8. Records, information, and items relating to control and use of IP address 69.5.116.44, including bills, mail envelopes, and payment information, including checking account, credit or debit card account information;

9. For any device whose seizure is otherwise authorized by this warrant:

a. Items 2 to 8 above;

b. Links to child pornography or to online locations where child pornography is stored;

c. Records and information showing access to and/or use of websites and applications used to commit the TARGET OFFENSES;

d. Records of Internet activity related, including logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, and records of internet protocol addresses used;

e. Names, addresses, contact information or lists of names, addresses or contact information, in any format, of those who may have been contacted in connection with the TARGET OFFENSES;

f. Evidence indicating whether and/or when child pornography was accessed and/or viewed by any user of the device;

g. Evidence of who used, accessed, owned, or controlled the device;

h. Evidence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

i. Evidence of the lack of such malicious software;

j. Evidence indicating how and when the device was accessed or used, and evidence indicating the geographic location of the device when it was accessed or used;

k. Evidence of the attachment to the device of other electronic devices or similar containers for electronic evidence;

l. Evidence of counter-forensic programs;

m. Passwords and encryption keys, and other access information that may be necessary to access the device;

n. Evidence of applications used to communicate with other individuals;

o. Evidence of applications used to access and view child pornography and/or visual depictions of minors engaging in sexually explicit conduct;

p. Any and all stored data related to the access, receipt, exchange, or creation of child pornography and/or visual depictions of minors engaging in sexually explicit conduct;

q. Any stored data consisting of evidence of access to child pornography and/or visual depictions of minors engaging in sexually explicit conduct, including Internet logs, Internet browser histories, website bookmarks;

r. Any software used to access hidden-service-websites;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, network hardware, routers and modems, cellular telephones and digital cameras.

The term "storage media" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular telephones capable of storage, floppy

disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

"Child Pornography" is defined in 18 U.S.C. § 2256(8), which includes as any visual depiction of sexually explicit conduct involving the use of a minor; a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct; or a visual depiction that has been created, adapted, or modified to appear than an identifiable minor is engaging in sexually explicit conduct.

"Visual depiction" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

Pursuant to Rule 41(e)(2)(B), it is authorized that electronically stored information may be imaged or copied. Consistent with Rule 41(e)(2)(B), the warrant is deemed executed once the subject computer has been physically seized, and that review of the contents of the subject computer is permitted at a later time.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Seth M. Fiore, a Special Agent of the Department of Homeland Security, Homeland Security Investigations, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a premises – including computers contained therein – located at [redacted] Burlington, Vermont (the "TARGET PREMISES"), as more fully described in Attachment A, which is incorporated herein by reference; and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, which is also incorporated herein by reference.

2. I have been employed as a Special Agent ("SA") of the Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI") since October 2009 and am currently assigned to the Office of the Resident Agent in Charge, Burlington, Vermont. As part of my duties, I am authorized to investigate violations of the laws of the United States, including but not limited to criminal violations relating to the sexual exploitation of children, child pornography, coercion and enticement, and transportation of minors, including but not limited to violations of Title 18, United States Code ("U.S.C.") §§ 2422, 2423, 2251, and 2252A (and conspiracy and attempt to commit the same) and I am authorized by law to request a search warrant.

3. As an SA in the Burlington HSI office, I frequently participate in the execution of search warrants involving child exploitation and pornography, and I work closely with both HSI and state and local forensic computer specialists throughout these investigations and prosecutions. I have received training in the area of child exploitation and child

pornography and gained experience in this investigative field through my work in numerous federal investigations related to child exploitation and child pornography. I have participated in numerous investigations involving individuals suspected of sexual exploitation of children, child pornography, coercion and enticement, and transportation of minors, and have written, obtained and coordinated the execution of search and arrest warrants pertaining to individuals involved in those and other federal offenses. I have prepared numerous affidavits in support of applications for search and arrest warrants which have resulted in orders being issued by judges, including authorization to search premises and computers, including cellular telephones, which have led to the convictions of numerous defendants for violations of federal laws, including violations relating to child exploitation and child pornography. In addition to my training in the area of child pornography, I have had, in my investigative capacity, the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) on digital forms of media, including computer media.

4. The statements in this affidavit are based in part on information provided by federal agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies; information gathered from the service of administrative subpoenas and summonses; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by federal agents/analysts and computer forensic professionals; and my experience, training, and background as a Special Agent with HSI. This affidavit is intended to show merely that there is sufficient probable cause for the issuance of the search warrant, and does not set forth all of my knowledge about this matter.

5. As described in further detail below, a Tor-hidden-service-website that was dedicated to child exploitative images and child pornography (hereinafter, "the CP Website"), was

accessed on multiple dates from April 18, 2019 through May 5, 2019 by an Internet-connected computer using Internet Protocol ("IP") address 69.5.116.44. IP address 69.5.116.44 is owned and operated by Burlington Telecom, an Internet service provider. IP address 69.5.116.44 has been assigned to the customer account of William KEVE since November 6, 2018, and I confirmed with Burlington Telecom that, on November 18, 2020, it was still active. The physical address associated with the customer account and the IP address is [redacted] Burlington, Vermont – the TARGET PREMISES and what I believe to be KEVE's home. On November 16, 2020, United States Postal Inspection Service electronically informed me that mail with the last name of Keve is delivered to [redacted] Burlington, Vermont.

6. A public records report for William KEVE, accessed through Consolidated Lead Evaluation and Response ("CLEAR"), a public records database that can be accessed and searched over the Internet, indicated that KEVE has been associated with the TARGET PREMISES since November 2018.

7. As described herein, I believe that a user of the Internet account at the TARGET PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described in the Probable Cause section of this affidavit and referred herein as the CP Website. There is probable cause to believe that a user of the Internet account at the TARGET PREMISES accessed the CP Website, as further described herein.

8. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 United States Code §§ 2252A(a)(2) and (b)(1) (receipt of child pornography), and §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), and attempt and conspiracy to commit those crimes, ("the

TARGET OFFENSES") have been committed at the TARGET PREMISES, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the TARGET PREMISES, described in Attachment A of this Affidavit. There is also probable cause to authorize the forensic examination of computers contained within the TARGET PREMISES for the purpose of identifying electronically stored data, particularly described in Attachment B.

DEFINITIONS

9. The following definitions apply to this Affidavit and Attachment B:

a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

c. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order

to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text- based online communications such as Internet forums and email.

d. "Cellular telephone (or mobile telephone, or wireless telephone, or smartphone)" as used herein, is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other cellular telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

e. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

f. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range

of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

g. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

i. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

j. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal- genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

k. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

The Tor Network

10. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

11. An IP address, as used herein, refers to a unique number used by a computer or other electronic device to access the Internet. An IP address (version 4) looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 01.234.01.234). Every computer or electronic device accessing the Internet must be assigned an IP address so that Internet traffic sent from or directed to that device may be properly directed from its source to its destination (akin to a telephone call being routed using a telephone number subscribed to a certain handset). Most ISPs, for example Burlington Telecom, control a certain range of IP addresses. IP addresses may be "static," if an ISP assigns a user's electronic device (e.g. a modem, router or computer) a particular IP address that is used each time the device accesses the Internet. IP addresses may also be "dynamic," meaning that the ISP assigns a different unique number to a device each time the device accesses the Internet using the ISP's service. ISPs typically maintain logs of the IP addresses assigned to users during sessions on particular dates and times.

12. The CP Website, further described below, operated on the Tor network, a computer network available to Internet users designed specifically to facilitate anonymous communication over the Internet. The Tor network is included in an area of the internet commonly referred to as the "dark web" because it is not publicly indexed on popular

search engine websites (e.g., Google). The Tor network attempts anonymity by routing Tor-user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through relay computers, traditional IP-address-based identification techniques are not effective.

13. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.[1] The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

14. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

15. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor

[1] Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

node from observing the content (but not the routing information) of other Tor users' communications. Similarly, this encrypted traffic can prevent law enforcement from observing the content of communications, even when judicially authorized (e.g., Title III authorization).

16. The Tor Project maintains a publicly available frequently asked questions ("FAQ") page, accessible from its website, with information about the Tor network, https://support.torproject.org/faq (last accessed on November 20, 2020). Within those FAQ, the Tor Project advises Tor users that it is possible for some entities to see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the network does not render a user's communications totally anonymous.

17. The Tor Network also makes it possible for users to operate websites, such as the CP Website, that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Hidden-services-websites often attempt anonymity to prevent their host servers from being seized or shut down by governments or law enforcement, whether or not they are used for illegal purposes (e.g., sites that host dissident political speech, sites that host child pornography). Like other websites, hidden-services-websites are hosted on computer servers that communicate through IP addresses. However, hidden-services-websites have unique technical features that attempt to conceal the computer server's location.

18. Unlike standard open-Internet websites (those publicly available on the surface web addresses using common Internet browsers like Microsoft Internet Explorer, e.g., justice.gov), a Tor-based web address is comprised of a series of at least 16, and as many as 56, algorithm-generated characters, for example, "asdlk8fs9dflku7f," followed by the suffix ".onion" (i.e., asdlk8fs9dflku7f.onion). Ordinarily, investigators can determine the IP

address of the computer server hosting an open-Internet website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing (akin to a phone book for registered open-Internet websites). Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor-hidden-service-website computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden-service-website.

19. Hidden-service-websites on the Tor Network are not "indexed" by search engines – such as Google – to anywhere near the same degree as websites that operate on the open-Internet. Accordingly, it is much more difficult to perform a Google-type search of Tor-hidden-service-websites than it is to search open-Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and child pornography websites they operate) must willfully seek out these websites and therefore keep, maintain, and use directory sites that advertise the web addresses of hidden-service-websites that contain child exploitation related content. Users utilize those directory sites to identify new hidden-service hosts of web forums, chat sites, image galleries, and file sharing pertaining to the sexual exploitation of children. While in operation, the web address for the CP Website was listed on one or more of these directory sites advertising hidden-service-websites dedicated to the sexual exploitation of children.

The CP Website

20. The CP Website was an online chat site whose primary purpose was to share and distribute child pornography. The advertisement and distribution of child pornography and child erotica were regular occurrences on this site. The CP Website started operating in approximately 2018 and appeared to cease operating in 2020.

21. On the front page of the site, the CP Website stated that the site was intended for users to "post links with good photos and videos" depicting "[o]nly GIRLS 4 to 14 years [old]." The site allowed users to engage in online chat with other users, either within chat rooms that were openly accessible to any user of the site, within rooms only accessible to particular users, or in one-to-one chats between two (2) users. Child pornography images and videos were trafficked through this chat site via the posting of web links within chat messages. Links allowed a user to navigate to another website, such as a file-hosting website, where images and/or videos were stored in order to download these images and videos. The CP Website provided its users with information about particular file hosting websites where users could upload digital files so that the files could then be shared, via links, with other users on the CP Website.

22. Entry to the site was obtained through free registration, as described below. On the registration page, it read, among other things, "No hurtcore, No gore, No zoo, No death, No toddlers." In my training and experience, "zoo" refers to pornography depicting bestiality, and "hurtcore" is a genre of child pornography that depicts violence, gore, torture, humiliation, or children in pain and distress. In addition, the registration page of the CP Website expressly contemplated the sharing of videos between members. Language on that page read, "Post links with good photos and videos (preview is required!)."

23. In order to pass through the registration page and gain access to the actual content of the CP Website, a prospective user must create a "Nickname" and a password which must be entered along with a Captcha. A "Captcha" is a randomly generated series of characters

designed to ensure that users of a website are human beings and not bots or other automated processes. Users are not required to enter any personally identifiable information, such as true names, emails, or phone numbers. The users may also pick a color for their posts (or one was randomly generated) and click "enter chat."

24. Upon initially creating a user account on the CP Website, a user was assigned the status of "Guest." As an unregistered user, the user receives the following message upon log in: "As it looks like you are not registered you may check our rules by sending to me word rules. There also will be some additional explanation of how to use this feature. News! We added feature of forum. Access by button at the bottom or just by this link: forum. this should make you be more happy of getting this message on entrance." Unregistered or "Guest" users could access the CP Website postings including postings that shared child pornography images.

25. In order to fully register an account, the user would need to obtain a promotion from "Guest" to "Registered Guest," which was done at the discretion of the CP Website staff. After an individual was promoted to a registered user account on the CP Website, a user must log in to that user account with the appropriate user-generated password in order to communicate via that user account on the CP Website. The CP Website users may register, log into, and access the CP Website through that user account using any computer or electronic device that was configured to use Tor routing/software.

26. As is common on these types of sites, the CP Website was administered and moderated by select CP Website users referred to as "Members" on the site. These users were promoted at the discretion of the site leadership. Promotions appeared to be made based on an individual's active participation on the site. Once promoted to a Member position, those users enforced the rules and assisted in the management of the site. That included controlling user membership using the "ban" and "kick" functions (which can limit or

eliminate a user's participation or account), promoting within the ranks of users, and moderating the public chatroom for content and user behavior.

27. CP Website Members periodically re-posted standard messages to the public chatroom of the CP Website iterating rules and procedures of the CP Website. For example, on or about May 28, 2019, a Member on the CP Website posted "CHAT RULES" in the public chatroom. That post contained statements in both Russian and English which included but was not limited to, "Follow the requests of the Members," "No hurtcore, No gore, No zoo, No death, No toddler," "Only GIRLS 5 to 13 years. Any language allowed," and "For RG (registered guests) the photo archive is available (the "links" button)."

28. Also on or about May 28, 2019, a Member posted "SECURITY INFORMATION" in the public chatroom. That post contained statements in both Russian and English which included but was not limited to the following:

- Set the Security Slider to HIGH Security Level
- Do Not Download if you are not using Encryption or Tails OS
- Read these manuals: □ Tails Guide & Tor Security Guide □
- Do Not Share any Identifying Information & NEVER Trust Anybody!
- Windows & OS X/MacOS are not safe for On topic
- Save files only to Encrypted Storage
- Windows Leaves traces you cannot clean without a Full disk wipe
- Linux offers Full Disk Encryption, Tails is Amnesic
- use VeraCrypt to create Hidden Encrypted Containers
- Open files when Offline to lower risk of malicious file causing trouble
- LEA & Antis are known to pose as parents and kids to trick you into revealing information to them, suspect everyone is LEA.
- LEA could be running this or any site at any time

- Always be conscious your messages may not be private

- Be Careful Paying for Anything, Bitcoin is not Anonymous by default!

29. When a user posted in the open chat, other users could see the name of the poster, what was posted and what time it was posted. Images posted to the site could be categorized or "tagged" by users based upon the image theme or characteristics. Those tags aided users in searching for specific types of content.

30. There was also an advertisement in the middle of the CP Website chat screen stating, "VISIT OUR SITES" and it featured four (4) links to other Tor sites. Each site had a short description along with a link to the Tor web address for the site. The descriptions stated: "Forum for boy-and girlovers" with a link to another website; "Chat for boylovers" – with a link to another website; "Girls pedo portal", and "only Ru". Based on my training and experience, I am aware that the reference to "only Ru" means that site is only for Russian speakers. Further, based on my training and experience, it is apparent that those websites were associated with each other.

31. The CP Website provided users with numerous links to image hosts where users could upload their digital images. For instance, on November 2, 2018, a CP Website user posted a hyperlink of a .jpeg file that linked to an image of a prepubescent girl having her underwear pulled down and a male penis resting on her inner thigh near her exposed vagina. In another instance, on March 1, 2019, a CP Website user posted a hyperlink of a .jpg file that linked to an image of a prepubescent female bent forward on what appeared to be a wooden chair with her back towards the camera. She was wearing a black and red skirt and no underwear. The female's anus and vagina were prominently exposed for the camera. Her face was turned to the side making it partially visible through her hair. The female had no pubic hair, was small in stature, and young facial features. Also, on May 27, 2019, a CP Website user posted a hyperlink to a .jpg image depicting a nude prepubescent female laying on a bed.

The image only showed the male's torso and upper leg from the side. The adult male was pushing his erect penis into the female's mouth.

32. Postings to the CP Website that were publicly available to any registered user at the time of posting were captured and archived for law enforcement review. Over 1,200,000 messages were posted on the CP Website between March 2018 and March 2020 when the site appeared to go offline. FBI SAs have accessed and downloaded child pornography files via links that were posted on the CP Website, in an undercover capacity.

33. A foreign law enforcement agency (herein referred to as "FLA") described the website as facilitating "the sharing of child sexual abuse and exploitation material, stipulating only girls aged 5 – 13.[2] Users were required to enter a username and password but these were only valid for that single login session" and provided further documentation naming the website as the CP Website, which the FLA referred to by its actual name.

34. While acting in an undercover capacity and observing the approximately over one (1) million files of suspected child pornography, law enforcement was able to access and download suspected child pornography files via links that were posted on the CP Website while it was still operating. Review of such postings included (but are not limited to) the following images within the CP Website:

a. **1556381394.jpg**: This is an image file which depicts what appears to be a fully nude, prepubescent, preteen girl laying on a comforter or bedding with her arms crossed, with a nude adult male touching his mostly erect penis and partially penetrating the girl vaginally.

b. **1544966953192.jpg**: This is an image file which depicts what appears to be a fully nude, prepubescent, preteen, very young girl sitting on a nude adult male's stomach, while the adult male appears to be lying on his back. The young girl's right hand is gripping the adult

[2] The range of ages of images in chats within the CP Website, as was reposted to the public chatroom by a CP Website Member, as described by FBI special agents appears to have been narrowed by one (1) year on each end of the age range from what FLA viewed on the front page of the CP Website, as described in paragraph 21.

male's erect penis. In the background appears to be two more naked girls, similar in age to the young girl sitting on the nude adult male's stomach.

c. **1544967068710.jpg**: This is an image file which depicts what appears to be a fully nude, prepubescent, preteen girl lying on a bed and looking up at a nude adult male sitting on the same bed with an erect penis. There appears to be a second, fully nude, prepubescent, preteen girl sitting on the same bed and looking at the camera which captured the image. In the background, there appears to be a third nude, young girl sitting up on the same bed.

Information Received from a Foreign Law Enforcement Agency

35. I am aware that U.S. and foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor-hidden-service-websites, including the CP Website described herein. These websites are globally accessible. Exploitative Tor-hidden-service-websites, and their users, can be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where geographically a particular exploitative Tor-hidden-service-website or user of that website is located. Accordingly, when a law enforcement agency obtains evidence that such an exploitative Tor-hidden-service-website or user may be located in another country, it is common practice for that law enforcement agency to share information with law enforcement agencies in the countries where the exploitative website site is located, or the country where the offender appears to reside, in accordance with the laws of each country.

36. In or around August 2019, an FLA known to U.S. law enforcement and with a history of providing reliable, accurate information in the past, notified U.S. law enforcement that FLA had determined that on April 18, 2019 at 14:45:04 Coordinated Universal Time ("UTC"), IP

address 69.5.116.44 was used to access online child sexual abuse and exploitation material via the CP Website which FLA named and described. FLA provided approximately six (6) additional dates and times IP address 69.5.116.44 was used to access the CP Website.

37. FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigation information with FLA, and FLA sharing criminal investigation information with U.S. law enforcement. This occurs across disciplines, including the investigation of crimes of children exploitation and child pornography. FLA advised U.S. law enforcement that it had obtained information related to access to the CP Website by IP address 69.5.116.44, as well as other IP addresses, through an independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain the IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

38. I am aware through my training and experience and consultation with other U.S. law enforcement agents that, as part of this investigation, leads and information provided by FLA regarding IP addresses that FLA advised were associated with access to Tor hidden-service child exploitation-related web and chat sites have:

a. led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse;

b. led to the seizure of evidence of child pornography trafficking and possession; and

c. been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

39. As described herein, the CP Website could not generally be accessed through the traditional Internet (i.e., using common web browsers including Microsoft Internet Explorer). Certain efforts needed to be employed to access the CP Website, including software installation and seeking out hidden-service-websites hosting child pornography. Only a user who had installed the appropriate Tor software on the user's computer (which may include smartphone cellular telephones) could access the CP Website. Even after connecting to the Tor network, a user would have to find the correct 16-or-56-character web address of the CP Website in order to access it. Hidden-service-websites on the Tor network are not "indexed" by search engines - such as Google - to anywhere near the same degree as websites that operate on the open-Internet. Many are not indexed by popular public search engines at all. Accordingly, it is much more difficult to perform a Google-type search of hidden-services-websites than it is to search open-Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain, and use directory sites that advertise the web addresses of hidden-services-websites that contain child exploitation related content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new Tor-hidden-service forums, chat sites, image galleries, and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (e.g., boys, girls, hurtcore). They also contain clickable hyperlinks to access those hidden sites and, as with other Tor-hidden-service-websites and, a user must find the

16-or-56 character web address for a directory website in order to access it. While it operated, the CP Website was listed on one or more of such directories of hidden sites advertising services dedicated to the sexual exploitation of children.

40. I am also aware - through HSI's consultation with agents from the Federal Bureau of Investigation ("FBI") - that the review of detailed user data related to another Tor-hidden-service child pornography website found that it was exceedingly rare for a registered website user to only access that website once and never return. FBI review of user data from that particular website found that less than two hundredths of one percent (0.02%) of user accounts registered an account on the Tor-hidden-service-website, accessed a message thread on the website, and then never returned to the website or never again logged in to the same account. Simply put, users of hidden-service child pornography websites seek out and find those sites that they enjoy and then return for continued use of the site. And where one child pornography website "goes down" and is no longer accessible (e.g., it is seized or disrupted by law enforcement), users of hidden-service child pornography websites will then seek out other similar sites, using directories and other means.

41. Accordingly, based on my training and experience and the information articulated herein, because accessing the CP Website required numerous affirmative steps by the user - including downloading Tor browser software, accessing the Tor network, seeking out the hidden-service web address for the CP Website, and then connecting to the CP Website via a Tor browser, it is extremely improbable that any user would simply stumble upon the CP Website, a hidden website, without understanding the clear purpose of the CP Website - to host and provide access of exploitative child pornographic material to users of the CP Website.

42. Accordingly, I submit that there is probable cause to believe that, based on the reasons described in this affidavit, any user who accessed the CP Website has, at a minimum,

knowingly and willfully accessed the CP Website with intent to access, view, and possess child pornography, and conspired with other individuals to do so.

IP Information Associated with the TARGET PREMISES

43. According to publicly available information, IP address 69.5.116.44 – used to access the CP Website on dates ranging from April 18, 2019 through May 5, 2019 – was determined to be owned and operated by ISP Burlington Telecom and subscribed to and used by KEVE.

44. On or about November 21, 2019, an administrative subpoena was served on Burlington Telecom for information related to the use of the IP address on April 18, 2019 at 14:45:04 UTC; April 24, 2019 at 17:27:15 UTC; April 26, 2019 at 14:42:31 UTC; April 27, 2019 at 15:14:17 UTC; May 1, 2019 at 19:17:20 UTC; May 3, 2019 at 13:53:39 UTC; and May 5, 2019 at 14:27:39. Burlington Telecom provided the following subscriber details:

- **Account Number**: 196022675
- **Name**: William Keve
- **Address**: [redacted] Burlington, VT 05401
- **Active Date**: November 6, 2018
- **Account Status**: Active
- **Phone**: 802-734-5860
- **Email**: WILLKEVE@gmail.com

45. In order to ensure KEVE's continued subscription to the account, I contacted Burlington Telecom and received, on November 18, 2020, an email from Burlington Telecom stating that account 196022675 was still active, KEVE was the subscriber, and the address was the same.

46. In sum, IP address 69.5.116.44 accessed the CP Website on April 18, 2019; April 24, 2019; April 26, 2019; April 27, 2019; May 1, 2019; May 3, 2019; and May 5, 2019. The IP address was assigned to KEVE's account then as it is now. I believe KEVE's Burlington

Telecom Internet account and the IP address associated with the TARGET PREMISES were used to access the CP Website.

USE OF COMPUTERS FOR CHILD PORNOGRAPHY

47. I have had training and experience in the investigation of computer-related crimes, including those involving child pornography. Based on my training and experience, I know the following:

a. Computers and digital technology, including cellular telephones and removable storage media, are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four (4) functions in connection with child pornography: production, communication, distribution, and storage.

b. Cellular telephones with cameras can take and save photographs or videos as a digital file that can be directly transferred to another computer via an Internet connection. Photos and videos taken on a cellular telephone may be stored to internal device memory or a removable memory card in the cellular telephone. Photos and video can also be transferred from computers to cellular telephones. The memory in cellular telephones, whether internal memory or removable memory cards, is often large enough to store thousands of high-resolution photographs or videos.

c. The ability of computers and cellular telephones to store images in digital form make the devices ideal repositories for child pornography. Storage media is any physical object upon which computer data can be recorded. The size of available memory for electronic storage media used in personal devices has grown tremendously within the last several years. Electronic storage media of various types - to include computer internal hard drives, external hard drives, CDs, DVDs, USB "thumb," "jump," or "flash" drives, and removable micro storage drives that can be contained inside of a cellular telephone (e.g., a Micro-SD card) - can store thousands of images or videos at very high resolution. It is extremely easy

for an individual to take a photograph or a video with a camera-bearing cellular telephone, and then save it (or any other files on the device) to any one of those media storage devices. Similarly, it is extremely easy for an individual to download a photograph or a video from a website and save it to internal device memory, or save or copy it (or any other files on the computer) to any one of those storage media. Some storage media, now not much bigger than the size of a small coin, can easily be concealed and carried on an individual's person. Cellular telephones, carried on an individual's person, act as electronic storage media themselves.

d. The Internet affords individuals several different venues for accessing, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

e. Individuals may also use online resources to store and retrieve child pornography, including services offered by Internet cloud storage providers (e.g., Google, Apple iCloud, Dropbox) and Internet email providers (e.g., Google Gmail, Yahoo! (Oath), and Microsoft Hotmail), or using the Tor network as described above. Online service providers allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage or email account from any computer with access to the Internet. However, even in cases where online storage is used, in most cases evidence of child pornography can also be found on the user's personal computer or cellular phone, as those devices can be used to access the online storage.

f. As is the case with most digital technology, a computer used for online communication can save or store communications and data. Storing this information can be intentional (e.g., saving an e-mail as a file on the device or saving a web address in "bookmarked" files). Digital information can also be retained unintentionally, with traces of the path of an electronic communication automatically stored in many places (e.g., temporary files). In

addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" (e.g., thumbnail photographs) in a web cache and history files of the web browser used.

48. Through my experience and training, and that of other HSI Special Agents, the following traits and characteristics are generally found to exist in cases involving individuals who collect images of child pornography, including digital images:

a. The majority of individuals who collect child pornography are individuals with a sexually-motivated attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography often seek out likeminded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, websites, mobile applications, email, email groups, bulletin boards, Internet chat programs, newsgroups, instant messaging, and other similar platforms.

c. Individuals who collect child pornography often collect and maintain points of contact to access and receive child pornography. In the digital context, individuals often maintain names, online user names, and addresses (including email addresses, web addresses and URLs) of persons who have advertised or otherwise made known on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral or exchange, or a means to trade, access or receive child pornography. These contacts may be maintained in personal devices (computers and cellular telephones) as saved

communications (e.g., message threads in an application or text messages), contacts, digital notes, bookmarks, word or text files, of in other digital formats.

d. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections from discovery, theft, and damage. I know from training and experience that such individuals have been known to maintain possession of their child pornography for years, or even decades. Collections are almost always maintained in the privacy and security of their homes or other secure locations, including personal devices, computers and cellular telephones. As described herein, as computing power has increased and the price of memory and storage has decreased, it is quite easy for individuals to maintain gigabytes of data containing thousands of images of child pornography.

CASE PROGRESSION AND PROBABILITY OF EXISTING CONTRABAND

49. According to FLA, the CP Website was last accessed by IP address 69.5.116.44 in the spring of 2019. Once United States law enforcement received the IP address from FLA, FBI issued an administrative subpoena, dated November 21, 2019, to Burlington Telecom. Once FBI received data related to IP address 69.5.116.44 from Burlington Telecom, it relayed data to HSI's Special Agent in Charge office in Boston, Massachusetts. After conducting precursory record checks, HSI Boston referred the investigation to HSI Burlington. On or around October 15, 2020, the investigation was assigned by HSI management to your affiant.

50. It is probable that computers located at the TARGET PREMISES will reveal evidence of commission of the TARGET OFFENSES, including evidence of a Tor browser and ongoing access to hidden-service-websites dedicated to child pornography. It is also probable that evidence of past storage of child pornography and past access to child pornography will be found. Forensic analysis of computers found at the TARGET

PREMISES are likely to find files and data 19-months old, or older, and this forensically recovered data from computers can reveal relevant evidence of an individual's commission of the TARGET OFFENSES.

51. Digital images and videos can easily and quickly be transferred between computers and storage media. Storage of these images, as described below, could occur to the memory of the computer used to access the Tor browser and hidden-service-websites, to discs or removable storage media, or to cloud-based storage solutions. Evidence of access to hidden-service-websites dedicated to child pornography could be readily apparent in computer logs and histories, or can be forensically recovered a computer's cache, as described below. Where computers are upgraded or replaced, it is now common for data and files to be transferred automatically from an "old" computer to a "new" computer (e.g., an Apple computer automatically moving a user's files from one device to another), or may be manually transferred from an "old" computer to a "new" computer. In my experience in digital investigations, it is common to find data and files on a computer that are older than a computer itself (e.g., photographs and video files dated before the "new" device was manufactured, transferred from an "old" device to a "new" device).

52. Where the crux of a search is for child pornography currently possessed by an individual - that is digital images and video - the target's primary computer, typically the one used to access the internet, is but one container to search. The ease by which digital files can be transferred and ubiquity of low-cost digital storage allow for many devices on which child pornography can potentially be stored. Further, I know from my training and experience that collectors of child pornography, knowing that they possess contraband, can be creative in their storage and secreting of child pornography - which in the past has included secreting removable storage media inside of a home, and maintaining old internal hard drives that are no longer inside of computers.

53. Where the search is also for evidence of past access to child pornography, forensic analysis of seized computers can reveal evidence through data that is both apparent and non-apparent. Manual review of a computer, or use of a forensic tool, may quickly reveal apparent evidence of past access to child pornography, whether months or years ago. For example, logs showing access to child pornography websites, or saved web addresses of child pornography websites would be this type of evidence. On the other hand, forensic analysis may also reveal non- apparent data, data that had been deleted or obfuscated by a user. Forensic tools may be able to recover data deleted months or even years ago, including photographs depicting child pornography. Forensic tools may also be able to recover data showing past access, and ongoing access, to child pornography websites, even if files were not intended to be downloaded by a user (e.g., the user viewed child pornography on a website but did not overtly take efforts to download the image file). For example, photographs viewed on a website may be stored a "thumbnail" images on a computer, without the user knowing that they are stored, showing prior access to a child pornography website months or years ago.

54. In my experience with HSI, I know that HSI investigators have been involved in child pornography investigations where evidence of access and possession of child pornography was forensically recovered from computers and the data was over 5-years-old.

55. I believe a search of the TARGET PREMISES, and analysis of computers contained therein, will reveal child pornography, and evidence of a user's access to the CP Website among other child pornography websites.

USE OF COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

56. As described above and in Attachment B, this application seeks permission to search for records that might be found on the TARGET PREMISES, in whatever form they are found, including data saved to computers. One form in which the records are likely to be found is

data stored on a computer's hard drive or other electronic storage media. Thus, this warrant would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, under Rule 41(e)(2)(B).

57. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on a device. This information can sometimes be recovered with forensics tools.

58. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of violations of the TARGET OFFENSES, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on computers found in the TARGET PREMISES because:

a. Data on the electronic storage media may provide evidence of a file that was once on the electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the electronic storage media that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, such as the attachment of USB flash storage devices or other electronic storage media, and the times the computer was in use. Computer file systems can record information about when the dates files were created and the sequence in which they were created, although this information can later be altered or falsified by a user.

b. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the electronic storage media until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the electronic storage media that is not currently being used by an active file - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media - in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but most computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." An Internet browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information logs which may reveal:

i. computer user account session times and durations;

ii. computer activity associated with user accounts;

iii. electronic storage media that connected with the computer;

iv. and the IP addresses through which the computer accessed networks and the Internet;

f. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both depict a particular location in a photograph and have geolocation information incorporated into its file data (e.g. a photograph clearly taken at City Hall in Burlington, Vermont with GPS coordinates of the location in Burlington where the photograph was taken incorporated into the photograph's metadata). Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage

media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user.

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic storage media, necessary to draw an accurate conclusion, is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on an electronic storage media. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

59. I know that when that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, contain data that is evidence of the crime, and serve as storage media for fruits of the crime (e.g., contraband child pornography). The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be electronic storage media for evidence of crime.

From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

Necessity of Seizing or Copying Entire Computers or Storage Media

60. Based on my knowledge, training, and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence - storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is

exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

c. Technical requirements - analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence, and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

61. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

62. The TARGET PREMISES may contain computer equipment whose use in the TARGET OFFENSES or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this

warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

63. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

Nature of Forensic Examination

64. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

65. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records, and information seized, copied, or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized, copied, or

disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

66. It is possible that the TARGET PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

67. *Manner of execution.* This warrant seeks only authorization to execute the search of the TARGET PREMISES during the day time – that is 6:00a.m. to 10:00p.m., local time.

CONCLUSION

68. Based on the foregoing, I submit that there is probable cause to believe that violations of the TARGET OFFENSES have been committed at the TARGET PREMISES. Since there has been no change of subscriber, William KEVE, to IP address 69.5.116.44 at the TARGET PREMISES since before someone accessed the now-defunct CP Website, and the current subscriber, William KEVE, still receives mail at the TARGET PREMISES, I believe there is probable cause that, based on the knowledge of how persons interested in viewing, exchanging, and collecting child pornography often keep their collections for months and years, that stored computer media may never truly be deleted from an electronic storage device, and that access to the CP Website took significant knowledge and intent, evidence of the TARGET OFFENSES still exists at the TARGET PREMISES. I respectfully submit that there is probable cause that the contraband, property, evidence, fruits, and instrumentalities of the TARGET OFFENSES, more fully described in Attachment B of this Affidavit, including child pornography and digital evidence of continued access to child pornography using the Internet, are located at the TARGET PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the TARGET

PREMISES described in Attachment A, authorizing the seizure and search of the items, including computers, described in Attachment B.

Respectfully submitted,

Seth M. Fiore
Special ~~Agent~~
Homeland Security Investigations

Subscribed and sworn to before me on Dec. 4th, 2020

HON. JOHN M. CONROY
UNITED STATES MAGISTRATE JUDGE

Exhibit 11

AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of
PREMISES LOCATED AT: [redacted], Barnhart Missouri, 63012 within the Eastern District of Missouri, a two-story structure with a tan siding and tan brick exterior, with black shutters, a three (3) car garage and a shingle-style roof. The numbers [redacted] are clearly displayed on the front porch post.
(SEE ATTACHMENT A.)

Case No. 4:20 MJ 3301 NCC

FILED UNDER SEAL

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Special Agent Daniel Root, FBI, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21, USC, § 2252(a)(2) and (b)(1)	receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct
21, USC, § 2252(a)(4)(b) and (b)(2)	possession of and access with intent to view a visual depictions of a minor engaged in sexually explicit conduct

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Daniel P. Root 11/12/2020
Applicant's signature

Special Agent Daniel Root, FBI
Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 40.

Date: November 12, 2020

Noelle C. Collins
Judge's signature

City and state: St. Louis, MO

Honorable Noelle C. Collins, U.S. Magistrate Judge
Printed name and title

AUSA: Jillian Anderson

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF: PREMISES LOCATED AT: [redacted] Barnhart Missouri, 63012 within the Eastern District of Missouri, a two-story structure with a tan siding and tan brick exterior, with black shutters, a three (3) car garage and a shingle-style roof. The numbers [redacted] are clearly displayed on the front porch post. (SEE ATTACHMENT A.)	No. 4:20 MJ 3301 NCC FILED UNDER SEAL SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Daniel Root, a Special Agent with the Federal Bureau of Investigation being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent (SA) of the Federal Bureau of Investigation (FBI) since January 2016, and am currently assigned to the St. Louis Division. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training provided by the FBI and through everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. During my time as a case agent on numerous complex investigations, I utilized a variety of investigative techniques to include: organizing and participating in physical surveillance; participating in undercover operations; serving search warrants; making arrests; and interviews involving defendants. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at [redacted] Barnhart, Missouri (the "SUBJECT PREMISES"), the content of electronic storage devices located therein, and any person located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § § 2251, 2252, and 2252A, which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252A(a)(1) and (b)(1) (transportation of child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign

commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. 18 U.S.C. § 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

e. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or

transported in or affecting interstate or foreign commerce by any means, including by computer.

f. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

g. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

h. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices);

peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i. "Wireless telephone or mobile telephone, or cellular telephone or cell phone or smartphone" as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

j. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

k. The "Domain Name System" or "DNS" is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

l. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

m. A "hidden service," also known as an "onion service," is website or other web service that is accessible only to users operating within the Tor anonymity network.

n. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

o. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

p. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

q. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

r. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

s. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form

t. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

u. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

v. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

w. The "Tor network" is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit."

x. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

y. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

z. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language

(HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein as the "TARGET WEBSITE."[1] There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE, as further described herein.

The Tor Network

7. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

8. The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

[1] The name of the TARGET WEBSITE is known to law enforcement. Investigation into the users of the website remains ongoing and disclosure of the name of the website would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

9. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.[2] The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

10. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

11. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

12. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

[2] Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

13. The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.
14. Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example "asdlk8fs9dflku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

Description of TARGET WEBSITE

15. The TARGET WEBSITE was an online bulletin board dedicated to the advertisement and distribution of child pornography that operated from approximately at least September 2016 to June 2019. In June of 2019, the computer server hosting the TARGET WEBSITE, which was located outside of the United States, was seized by a foreign law enforcement agency.
16. A review of the initial TARGET WEBSITE page revealed it was a message board web page that contained a search bar, and showcased two hyperlinks titled, "Announcements" and "Important Information." Located below the title were hyperlinks including those entitled

"Quick Links," "Home," "Board Index," "Login," and "Register." As of June 2019, the website had over 820,000 members and over 81,000 postings.

17. Upon accessing the "Announcements" hyperlink of the TARGET WEBSITE, the following message was displayed in message board form, "Welcome, Please read before registering" which was dated July 1, 2016. Upon accessing the aforementioned hyperlink, the message read, "Welcome abusers and abusees and those that enjoy watching. This website was created to host videos, photos and discussions of 18 (twinks) and younger of Hurtcore materials (videos & pictures) as well as discussion of such." Based on my training and experience, I know that Hurtcore refers to violent pornography. The message continued, "PS Please register to see all the forums, and use strong password for user profile."

18. Upon accessing the "Register" link of the TARGET WEBSITE, it was revealed that users would complete a "Username," "Password," "Confirm password," "Language," and "My timezone," fields, as well as a "Confirmation of Registration" code. Upon entering the TARGET WEBSITE, sections and forums for posting to the website included "HURTCORE Toddlers Videos (Ages 0-5)," "Preteen/Hebe Children Videos (Ages 6-13)," "Teens Videos (Ages 14+)," "Toddlers Images (Ages 0-5)," "Preteen/Hebe Children Images (Ages 6-13)," and "Teens Images (Ages 14+)." Based on my training and experience, I know that "Hebe" is a reference to a "hebephile," which is a person with a persistent sexual interest in pubescent minor children. Another forum was named "GORE/DEATH" which included sub-forms for "Toddlers (Ages 0-5)," "Preteen/Hebe Children (Ages 6-13)" and "Teens (Ages 14+)." An additional section of the website called "The Team" listed the usernames of two website "Administrators" and five "Global Moderators." The TARGET WEBSITE also contained a private message feature that was available, allowing users to send private messages to each other.

19. On June 23, 2016, a website administrator posted a topic entitled "Board Rules" in the "Important Information" forum which contained the following explanation of the website: Rules are simple all material must be related to Hurtcore content. What is Hurtcore content? It is rape, fighting, wrestling, bondage, spanking, pain, mutilation, gore, dead bodies, and etc. (no limits) Why does this place exist? There was a need and since society thinks I am worst than any abuser or creator of Hurtcore content, I decided to create this place for those who like

it and want to share. Besides I am the mischievous god. It is up to you to make this the best Hurtcore board there is. So please upload whatever you can so that it can be shared.

20. A review of the "Toddlers Videos," "Preteen/Hebe Children," "Toddlers Images," and "Gore/Death" forums and subforums, as well as additional forums, within the various above sections revealed they contained numerous pages of topics. Each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the thread below it. Typical posts appeared to contain text, images, thumbnail previews of images, links to external sites with compressed files (such as ".rar"), or replies to previous posts.

21. A review of topics within these sections revealed numerous posts containing images and/or videos depicting child pornography and child erotica of prepubescent males, females, toddlers, and infants; including those depicting anal, vaginal, and oral penetration. Additionally, these sections revealed numerous posts containing images and/or videos depicting child pornography involving gore and sometimes death. Examples of these are as follows:

22. On October 9, 2016, a website user posted a topic entitled "Fuck the newborn. Real fuck!" in the "Hurtcore/Toddlers Images/Girls" forum that contained nine images depicting child pornography and child erotica of a prepubescent female infant. One of these images depicted a naked female infant lying on her back with her legs spread apart, exposing her vagina, with a gloved adult finger inserted into her anus. A male's penis was pressed against her vagina and the head of the penis inserted into her mouth. A brown liquid substance, appearing to be the infant's feces are seen smeared around her anus.

23. On November 5, 2016, a website user posted a topic entitled "BabyHee 1yo (one of full version)" in the "HurtCore/Toddlers Videos/Boys" forum that contained images depicting child pornography and torture of a prepubescent male, who was completely naked and tied down with rope on the side of a bath tub. Among other things, the images depicted an adult male defecating on the chest and urinating in the mouth of the prepubescent male.

Evidence Related to Identification of Target that Accessed TARGET WEBSITE

24. I am aware that U.S. as well as foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the website(s) described herein. Those websites are globally accessible. The websites and their users may therefore be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the website is located or the offender appears to reside, in accordance with each country's laws.

25. In August 2019, a foreign law enforcement agency (referenced herein as "FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that FLA determined that on May 24, 2019, IP address 76.253.61.232 "was used to access online child sexual abuse and exploitation material" via a website that the FLA named and described as the TARGET WEBSITE. FLA described the website as having "an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children," stated that "[u]sers were required to create an account (username and password) in order to access the majority of the material," and provided further documentation naming the website as the TARGET WEBSITE, which the FLA referred to by its actual name.

26. FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law

enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

27. I am aware through my training and experience and consultation with other U.S. law enforcement agents that tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites have: (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

28. As described herein, the TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software on the user's computer could access the "TARGET WEBSITE." Even after connecting to the Tor network, however, a user would have to find the 16-or-56-character web address of the TARGET WEBSITE in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory website in order to access it. While it operated, the web address for the website described herein was listed on

one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

29. Accordingly, based on my training and experience and the information articulated herein, because accessing the TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

30. Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed the TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so.

Identification of SUBJECT PREMISES

31. On May 24, 2019, TARGET WEBSITE was accessed at 01:34:38 UTC from IP address 76.253.61.232.

32. According to publicly available information, IP address 47.24.167.115 was owned/operated by AT&T Communications, Inc.

33. On November 22, 2019, an administrative subpoena was issued to AT&T in regard to the pertinent IP address. A review of the results obtained on November 25, 2019, identified the following account holder and address:

Name: Tracey Lawson
Address: [redacted] Barnhart, MO 63012
Telephone: 314-541-0367

34. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for [redacted] Barnhart, MO. This search revealed that [redacted], Barnhart, MO was a single family residence, owned by **Brent M. and Tracey L Lawson.** These public records indicated that **BRENT M. LAWSON**, date of birth [redacted]/1976, and **TRACEY L LAWSON,** date of birth xx/xx/70 currently reside at the SUBJECT PREMISES and that they have owned/lived at this address since April of 2015.

35. A check with the Department of Motor Vehicles on or about August 19, 2020, revealed that BRENT LAWSON'S driver's license lists the SUBJECT PREMISES as his current address, and he has a vehicle registered with the State of Missouri that he owns and that is also registered to the SUBJECT PREMISES.
36. On or about August 13, 2020, a representative from Ameren indicated that electric service is currently being provided to **BRENT LAWSON** at the SUBJECT PREMISES.
37. Surveillance of the SUBJECT PREMISES on or about August 18, 2020, identified a silver Toyota Highlander bearing Missouri license plate NC3-M5A, parked in the driveway in front of the residence, and a silver 2004 GMC Yukon bearing Missouri license plate GF9-S0E also parked in the driveway. The Toyota Highlander was determined to be registered to **TRACEY LAWSON**. The GMC Yukon was determined to be registered to **BRENT LAWSON**.
38. Further research indicated that **BRENT MICHAEL LAWSON** is a registered sex offender per records maintained by the Missouri State Highway Patrol. His address is listed in the sex offender registry as [redacted], Barnhart MO, for both work and home addresses. Vehicles registered to him on the sex offender registry are a 2004 Yukon with plate GF9-S0E, a 2019 Kia with plate XD1-D1J, and a 2017 Highlander with plate NC3-M5A. According to public records available via the Public Access to Court Electronic Records (PACER) website, his obligation to register stems from a conviction on April 22, 2004, in the U.S. District Court for the E.D. of Missouri, for the offenses of Transportation of Child Pornography in violation of Title 18, United States Code, Section 2252(a)(1); Attempted Receipt of Child Pornography in violation of Title 18, United States Code, Section 2252A(a)(2); and Possession of Child Pornography in violation of Title 18, United States Code, section 2252A(a)(5)(B), for which **BRENT MICHAEL LAWSON**, was sentenced by the Hon. Judge Stephen N. Limbaugh to sixty months of imprisonment followed by three years of supervised release.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

39. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or

smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

40. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website.

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

41. Based on all of the information contained herein, I believe that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access online child sexual abuse and exploitation material via a website. In particular, the target of investigation obtained and used Tor network software, found the web address for TARGET WEBSITE, and accessed online child sexual abuse and exploitation material via the TARGET WEBSITE.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

42. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

44. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as

the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an

incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or

received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

45. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading

filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

46. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

47. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require

techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

48. This warrant permits law enforcement to compel **BRENT MICHAEL LAWSON** to unlock any DEVICES owned or used by him requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that

match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when

the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of **BRENT MICHAEL LAWSON** to the fingerprint scanner of the DEVICES found at the PREMISES;
(2) hold the DEVICES found at the PREMISES in front of the face of **BRENT MICHAEL LAWSON** and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face of **BRENT MICHAEL LAWSON** and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that **BRENT MICHAEL LAWSON** state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel **BRENT MICHAEL LAWSON** to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

49. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

50. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

I state under the penalty of perjury that the foregoing is true and correct.

Daniel P. Root 11/12/2020

DANIEL ROOT
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 40.this 12th day of NOVEMBER, 2020.

Honorable Noelle C. Collins
UNITED STATES MAGISTRATE JUDGE

4:20 MJ 3301 NCC
ATTACHMENT A
DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire premises located at [redacted], Barnhart, Missouri, and any person located at the SUBJECT PREMISES.

A two-story structure with a tan siding and tan brick exterior, with black shutters, a three (3) car garage and a shingle-style roof. The numbers [redacted] are clearly displayed on the front porch post.



4:20 MJ 3301 NCC

ATTACHMENT B
ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § § 2251, 2252 and 2252A

a. Computers or storage media used as a means to commit the violations described above.

b. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

c. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

d. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

e. evidence of the lack of such malicious software;

f. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

g. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

h. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

i. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

j. evidence of the times the COMPUTER was used;

k. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

l. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

m. records of or information about Internet Protocol addresses used by the COMPUTER;

n. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; andcontextual information necessary to understand the evidence described in this attachment.

o. Routers, modems, and network equipment used to connect computers to the Internet.

p. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

q. Records, information, and items relating to violations of the statutes described above including:

r. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, [redacted], Barnhart, MO, including utility and telephone bills, mail envelopes, or addressed correspondence;

s. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

t. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

u. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel **BRENT MICHAEL LAWSON** to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the DEVICE(S) known to be used by **BRENT MICHAEL LAWSON** that are found at the PREMISES, and

(b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that **BRENT MICHAEL LAWSON** state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Exhibit 12

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PANAMA CITY DIVISION

IN THE MATTER OF THE SEARCH OF [redacted], CHIPLEY, FLORIDA 32428	Case No. 5:20-mj-44-MJF **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Lawrence P. Borghini, a Special Agent with the Federal Bureau of Investigation ("FBI") being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") of FBI, since April 14, 1996, and am currently assigned to the Jacksonville Division, Panama City Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training provided by the FBI and everyday work relating to conducting these types of investigations. I have received specialized training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Consequently, I am familiar with the ways in which these individuals/organizations

operate their illegal enterprise, including, but not limited to, their use of computers, cellular telephones, media storage and current technology to conduct their transactions.

2. Within the scope of my duties, I have been assigned investigations involving individuals and criminal enterprises engaged in child pornography and child exploitation. I have personally participated in court authorized wiretaps, physical surveillances, the execution of search warrants, arrest warrants and interviews of individuals engaged in child pornography and child exploitation. I have also been involved in an number of undercover operations specifically targeting individuals engaged in child pornography and child exploitation. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2252A(a)(2) and (a)(5), and I am authorized by law to request a search warrant.

3. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at [redacted], Chipley, Florida, (the "SUBJECT PREMISES"), the content of electronic storage devices located therein, and any person located at the SUBJECT PREMISES, for contraband and evidence, fruits,

and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2) and (a)(5), which items are more specifically described in **Attachment B** of this Affidavit.

4. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct) and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign

commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent

between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual

depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

g. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

h. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units,

internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. The "Domain Name System" or "DNS" is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

k. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

l. A "hidden service," also known as an "onion service," is website or other web service that is accessible only to users operating within the Tor anonymity network.

m. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to

the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

p. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

q. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

r. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

s. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

t. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

u. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

v. The "Tor network" is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit."

w. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or

typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

x. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

y. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

7. A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein as the "TARGET

WEBSITE."[1] There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE, as further described herein.

The Tor Network

8. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

9. The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts

[1] The name of the TARGET WEBSITE is known to law enforcement. Investigation into the users of the website remains ongoing and disclosure of the name of the website would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

10. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.[2] The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

11. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information

[2] Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

12. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

13. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the

question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

14. The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

15. Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example "asdlk8fs9dflku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public

lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

Description of TARGET WEBSITE

16. The TARGET WEBSITE was an online bulletin board dedicated to the advertisement and distribution of child pornography that operated from approximately at least September 2016 to June 2019. In June of 2019, the computer server hosting the TARGET WEBSITE, which was located outside of the United States, was seized by a foreign law enforcement agency.

17. A review of the initial TARGET WEBSITE page revealed it was a message board web page that contained a search bar, and showcased two hyperlinks titled, "Announcements" and "Important Information." Located below the title were hyperlinks including those entitled "Quick Links," "Home," "Board Index," "Login," and "Register." As of June 2019, the website had over 820,000 members and over 81,000 postings.

18. Upon accessing the "Announcements" hyperlink of the TARGET WEBSITE, the following message was displayed in message board form, "Welcome, Please read before registering" which was dated July 1, 2016. Upon accessing the aforementioned hyperlink, the message read, "Welcome abusers and abusees and those that enjoy watching. This website was created to host videos, photos and discussions of 18 (twinks) and younger of Hurtcore materials (videos & pictures) as well as discussion of such." Based on my training and experience, I know that Hurtcore refers to violent pornography. The message continued, "PS Please register to see all the forums, and use strong password for user profile."

19. Upon accessing the "Register" link of the TARGET WEBSITE, it was revealed that users would complete a "Username," "Password," "Confirm password," "Language," and "My timezone," fields, as well as a "Confirmation of Registration" code. Upon entering the TARGET WEBSITE, sections and forums for posting to the website included "HURTCORE Toddlers Videos (Ages 0-5)," "Preteen/Hebe Children Videos (Ages 6-13)," "Teens Videos (Ages 14+)," "Toddlers Images (Ages 0-5)," "Preteen/Hebe Children Images (Ages 6-13)," and "Teens Images (Ages 14+)." Based on my training and experience, I know that "Hebe" is a reference to a "hebephile," which is a person with a persistent sexual interest in pubescent minor children. Another forum was named "GORE/DEATH"

which included sub-forms for "Toddlers (Ages 0-5)," "Preteen/Hebe Children (Ages 6-13)" and "Teens (Ages 14+)." An additional section of the website called "The Team" listed the usernames of two website "Administrators" and five "Global Moderators." The TARGET WEBSITE also contained a private message feature that was available, allowing users to send private messages to each other.

20. On June 23, 2016, a website administrator posted a topic entitled "Board Rules" in the "Important Information" forum which contained the following explanation of the website:

> Rules are simple all material must be related to Hurtcore content. What is Hurtcore content? It is rape, fighting, wrestling, bondage, spanking, pain, mutilation, gore, dead bodies, and etc. (no limits) Why does this place exist? There was a need and since society thinks I am worst than any abuser or creator of Hurtcore content, I decided to create this place for those who like it and want to share. Besides I am the mischievous god. It is up to you to make this the best Hurtcore board there is. So please upload whatever you can so that it can be shared.

21. A review of the "Toddlers Videos," "Preteen/Hebe Children," "Toddlers Images," and "Gore/Death" forums and subforums, as well as additional forums, within the various above sections revealed they contained numerous pages of topics. Each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the

top of the page, with any corresponding replies to the original post included in the thread below it. Typical posts appeared to contain text, images, thumbnail previews of images, links to external sites with compressed files (such as ".rar"), or replies to previous posts.

22. A review of topics within these sections revealed numerous posts containing images and/or videos depicting child pornography and child erotica of prepubescent males, females, toddlers, and infants; including those depicting anal, vaginal, and oral penetration. Additionally, these sections revealed numerous posts containing images and/or videos depicting child pornography involving gore and sometimes death. Examples of these are as follows:

23. On October 9, 2016, a website user posted a topic entitled "Fuck the newborn. Real fuck!" in the "Hurtcore/Toddlers Images/Girls" forum, that contained nine images depicting child pornography and child erotica of a prepubescent female infant. One of these images depicted a naked female infant lying on her back with her legs spread apart, exposing her vagina, with a gloved adult finger inserted into her anus. A male's penis was pressed against her vagina and the head of the penis inserted into her mouth. A brown liquid substance, appearing to be the infant's feces are seen smeared around her anus.

24. On November 5, 2016, a website user posted a topic entitled "BabyHee lyo (one of full version)" in the "HurtCore/Toddlers Videos/Boys" forum that contained images depicting child pornography and torture of a prepubescent male, who was completely naked and tied down with rope on the side of a bath tub. Among other things, the images depicted an adult male defecating on the chest and urinating in the mouth of the prepubescent male.

Evidence Related to Identification of Target

That Accessed TARGET WEBSITE

25. I am aware that U.S. as well as foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the website(s) described herein. Those websites are globally accessible. The websites and their users may therefore be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the website is located or the offender appears to reside, in accordance with each country's laws.

26. In August 2019, a foreign law enforcement agency (referenced herein as "FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that FLA determined that on April 12, 2019 at 10:51:20 (UTC), IP address 104.191.59.32 "was used to access online child sexual abuse and exploitation material" via a website that the FLA named and described as the TARGET WEBSITE.

27. FLA described the website as having "an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children," stated that "[u]sers were required to create an account (username and password) in order to access the majority of the material," and provided further documentation naming the website as the TARGET WEBSITE, which the FLA referred to by its actual name.

28. FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully

authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

29. I am aware through my training and experience and consultation with other U.S. law enforcement agents that tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites have: (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

30. As described herein, the TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software on the user's computer could access the "TARGET WEBSITE." Even after connecting to the Tor network, however, a user would have

to find the 16-or-56-character web address of the TARGET WEBSITE in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory website in order to access it. While it operated, the web address for the website described herein was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

31. Accordingly, based on my training and experience and the information articulated herein, because accessing the TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

32. Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed the TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so.

Identification of SUBJECT PREMISES

33. According to publicly available information, IP address 104.191.59.32 which was used to access TARGET WEBSITE on April 12, 2019, was registered to AT&T.

34. On or about February 20, 2020, an administrative subpoena was issued to AT&T in regard to the pertinent IP address. Shortly thereafter, a review of the results obtained identified the following account holder and address, which is the address of the SUBJECT PREMISES: Cynthia Duffy, [redacted], Chipley, Florida 32428.

35. An Accurint database search, that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information, was conducted for [redacted], Chipley, Florida 32428. The search identified Cynthia Duffy and Christopher Coy Duffy as possible residents.

36. A check of the Washington County Property Appraiser's website shows that Cynthia Dianne Duffy is the owner of the parcel of land and two bedroom, two bath, 1,067 square foot residence located at [redacted], Chipley, Florida 32428. Cynthia Dianne Duffy has owned the property since 2005. A homestead exemption is being claimed for the property.

37. A search of the Florida Driver License and Vehicle Information Database (DAVID) for the SUBJECT PREMISES address revealed that an individual named Christopher Coy Duffy with a date of birth of [redacted] 1982, and Cynthia Dianne Duffy with a date of birth [redacted], 1952, list the SUBJECT PREMISES address as their residence. Within the documents section of DAVID for Christopher Coy Duffy was a birth certificate showing Cynthia Dianne Duffy as his mother. Christopher Coy Duffy has a current vehicle registration for a 2005 green Jeep Wrangler bearing Florida license plate DUFFLLC listing the SUBJECT PREMISES address.

38. A search of the Florida Department of State Division of Corporations lists DUFF, LLC's principal and mailing addresses as [redacted], Sunny Hills, Florida 32428 (the SUBJECT PREMISES)[3] and Christopher C, Duffy as the owner. DUFF, LLC filed Articles of Organization with the State of Florida on September 16, 2013, and had shown the SUBJECT PREMISES address as its' principal address and mailing address each year. DUFF, LLC is currently shown as inactive as having been administratively dissolved for annual report on September 27, 2019.

39. Surveillance of the SUBJECT PREMISES on May 4, 2020, revealed a single story blue residence with a Keystone Residence travel trailer located in the back yard. Surveillance cameras were mounted on the exterior of travel trailer. A green Jeep Wrangler bearing Florida license plate "DUFFLLC" was parked in close proximity to the travel trailer. The travel trailer had various items scattered under and around it indicating that it had been in place for some time and was occupied.

40. During the surveillance, in an effort to gain additional information regarding any potential wireless networks at the SUBJECT PREMISES, the Wi-Fi connection settings of a law enforcement wireless device was queried from the street

[3] Sunny Hills is a residential community located in Washington County, Florida. The mailing address for the Sunny Hills area is Chipley, Florida.

directly in front for the SUBJECT PREMISES. It was noted that there were three (3) wireless networks in the area and all of them were secured. Accordingly, to use any of them to access the Internet, a user would likely have to know the encryption key or password for that particular network. Based on the signal strength of the wireless networks, as well as my training and experience and information relayed to me by agents, I believe that the wireless router at the SUBJECT PREMISES is likely generating a secured wireless network. Furthermore, the names of the wireless networks observed were ATT976, IBR900-548 and IBR900-548-5g. Each of the wireless networks displayed a signal strength bar next to it with a closed lock indicating the that wireless network was secured. It should be noted that one of the wireless networks observed and the IP address 104.191.59.32 used to access TARGET WEBSITE on April 12, 2019, was registered to AT&T. As explained above, I know, from my training and experience and information relayed to me by agents, that wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime.

41. A check of open source information from the Internet regarding Christopher Coy Duffy revealed he had been arrested by the Washington County Sheriff's Office after being accused of sexually abusing a six-year-old child in

Washington County. According to the reports, Christopher Coy Duffy had forced the victim to perform sexual acts on him and touched the child's genitals.

42. A check of the records for the Clerk of the Courts for Washington County, Florida, shows Christopher Coy Duffy named as a defendant in case number 672019CF00293A in which he was charged with violating § 794.011(2)(a), Florida Statute, Sexual Battery on a Person less that 12 Years of Age. Christopher Coy Duffy was arrested on June 21, 2019. Bond was posted the following day. According to documents filed in the matter, the alleged activity occurred between the dates of December 1, 2018, and January 31, 2019. According to the victim, the sexual assault occurred in a camper when the victim was staying with Christopher Coy Duffy. Christopher Coy Duffy's address in the state case is listed as [redacted] Chipley, Florida 32428 (the SUBJECT PREMISES). The matter is currently pending with a next scheduled court date of June 15, 2020.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

43. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online

storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be

automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

44. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website.

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion

pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical

and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that

evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

45. Based on all of the information contained herein, I believe that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access online child sexual abuse and exploitation material via a website. In particular, the target of investigation obtained and used Tor network software, found the web address for TARGET WEBSITE, and accessed online child sexual abuse and exploitation material via the TARGET WEBSITE.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

46. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

47. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic

evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

48. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word

processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or

controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The

existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is

possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From

my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

49. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized

equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the

use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

50. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly.

Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

51. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many

parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

52. This warrant permits law enforcement to compel Christopher Coy Duffy to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is

registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding

the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the

DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be

unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Christopher Coy Duffy to the fingerprint scanner of the DEVICES found at the PREMISES; (2) hold the DEVICES found at the PREMISES in front of the face of Christopher Coy Duffy and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face of Christopher Coy Duffy and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that Christopher Coy Duffy state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel Christopher Coy Duffy to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

53. Furthermore, law enforcement personnel will compel the use of Christopher Coy Duffy's biometric features only if (a) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at time of the compulsion, law enforcement personnel has (b) reasonable suspicion that

Christopher Coy Duffy has committed a criminal act that is the subject matter of the requested search warrant, and (c) reasonable suspicion that Christopher Coy Duffy's biometric features will unlock the respective device.

CONCLUSION

54. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

55. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Lawrence P. Borghini
Special Agent
Federal Bureau of Investigation

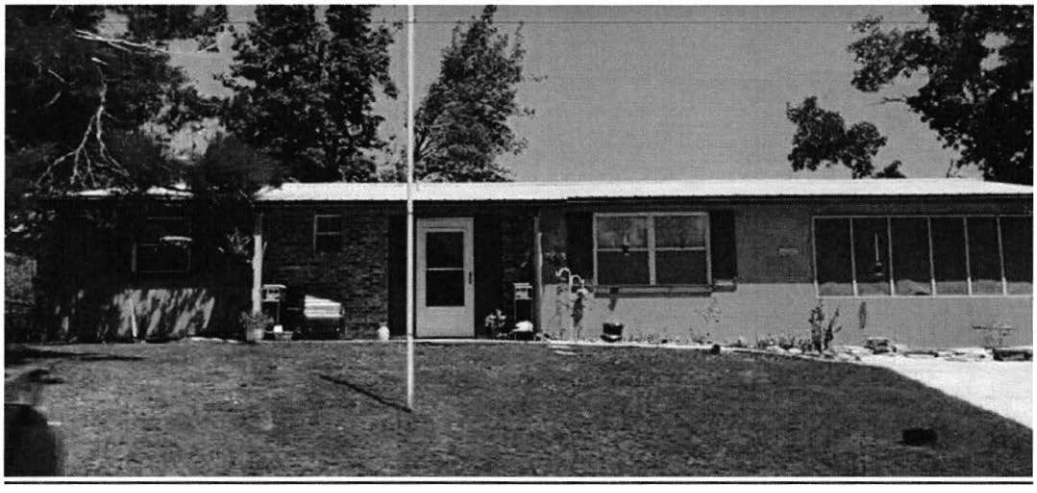
Sworn and subscribed before me this 6th day of May, 2020.

/s/ Michael J. Frank
Michael J. Frank
United States Magistrate Judge

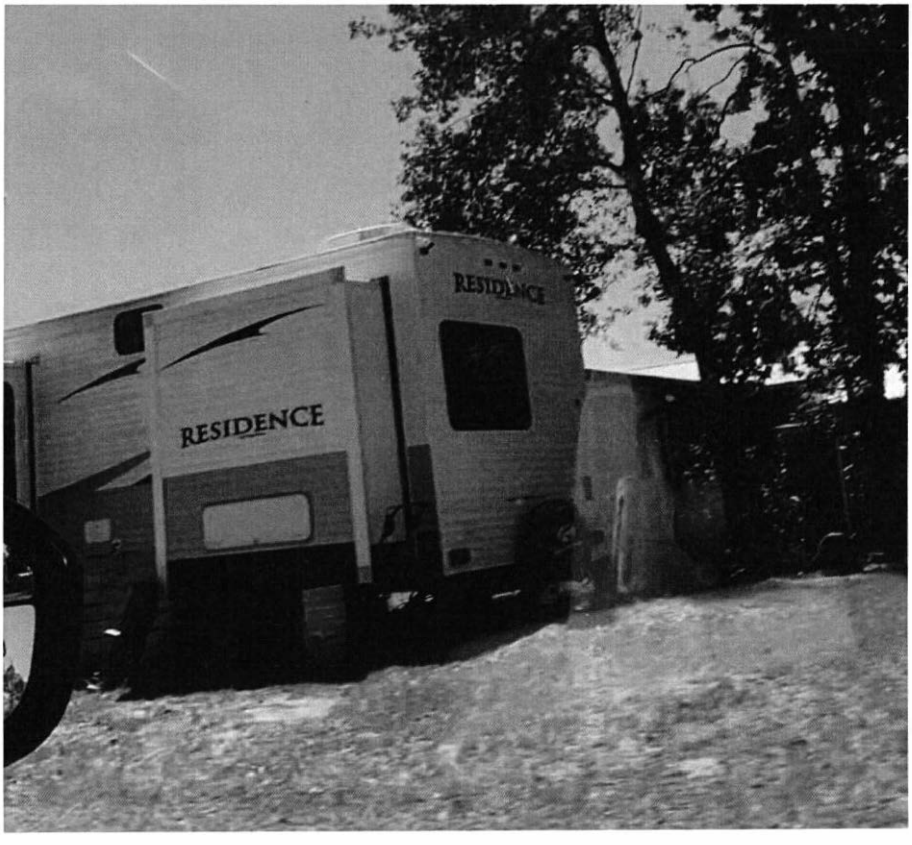
ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at [redacted], Chipley, Florida 32428, including the residential building, travel trailer, outbuildings, and any appurtenances thereto (the SUBJECT PREMISES), and any person located at the SUBJECT PREMISES.






RESIDENCE
RESIDENCE



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2252A(a)(2) and (a)(5):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, [redacted], Chipley, Florida 32428, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel Christopher Coy Duffy to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the DEVICES found at the PREMISES, and

(b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that Christopher Coy Duffy state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES. Furthermore, law enforcement personnel will compel the use of Christopher Coy Duffy's biometric features only if (a) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at time of the compulsion, law enforcement personnel has (b) reasonable suspicion that Christopher Coy Duffy has committed a criminal act that is the subject matter of the requested search warrant, and (c) reasonable suspicion that Christopher Coy Duffy's biometric features will unlock the respective device.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order

to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Exhibit 13

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Maine

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Entire property located at [redacted],
Gardiner, Maine 04345,
Attachment A

Case No. 1:20-mj-00255-JCN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give*
Entire property located at [redacted], Gardiner, Maine 04345, more fully described in Attachment A

located in the _____ District of Maine , there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252A(a)(5)(B), (b)2	Possession of and access with intent to view child pornography.

The application is based on these facts:
See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Chase Ossinger, Special Agent, HSI
Printed name and title

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedure

Date: Sep 08, 2020,

Judge's signature

City and state: Bangor, Maine

John C Nivson U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Chase Ossinger, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") of U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), since 2009, and am currently assigned to HSI Bangor, Maine. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) I have been the case agent on child exploitation cases that have resulted in arrests, prosecution, and convictions for possession, distribution, and production of child pornography. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at [redacted], Gardiner, Maine 04345 (the "SUBJECT PREMISES"), the content of electronic storage devices located therein, and any person located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. 2252A, which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. This Affidavit sets forth facts I believe establish probable cause to conclude that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured and provides members with the ability to view

postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

g. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

h. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output

devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. The "Domain Name System" or "DNS" is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

k. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

l. A "hidden service," also known as an "onion service," is website or other web service that is accessible only to users operating within the Tor anonymity network.

m. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices

on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

p. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

q. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

r. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

s. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

t. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

u. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

v. The "Tor network" is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit."

w. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

x. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of

conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

y. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein as the "TARGET WEBSITE."[1] There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE, as further described herein.

The Tor Network

7. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content

[1] The name of the TARGET WEBSITE is known to law enforcement. Investigation into the users of the website remains ongoing and disclosure of the name of the website would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

8. The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

9. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.[2] The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

10. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

[2] Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

11. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

12. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

13. The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

14. Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example "asdlk8fs9dflku7f.," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server

hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

Description of TARGET WEBSITE

15. The TARGET WEBSITE is an active online chat site whose primary purpose is to share and distribute child pornography. The advertisement and distribution of child pornography and child erotica are regular occurrences on this site. The TARGET WEBSITE started operating in approximately 2018.

On the front page of the site, it states that the site is intended for users to "post links with good photos and videos" depicting "[o]nly BOYS 5 to 13 years [old]." The site allows users to engage in online chat with other users, either within chat rooms that were openly accessible to any user of the site, within rooms only accessible to particular users, or in one-to-one chats between two users. Child pornography images and videos are trafficked through this chat site via the posting of web links within chat messages. Links allow a user to navigate to another website, such as a file-hosting website, where images and/or videos were stored in order to download these image and videos. The TARGET WEBSITE provides its users with information

about particular file hosting websites where users could upload digital files so that the files could then be shared, via links, with other users on the TARGET WEBSITE.

Entry to the site is obtained through free registration, as described below. On the registration page, it reads, among other things, "No hurtcore, No gore, No zoo, No death, No toddlers." In my training and experience, "zoo" refers to pornography depicting bestiality, and "hurtcore" is a genre of child pornography that depicts violence, gore, torture, humiliation, or children in pain and distress. In addition, the registration page of the TARGET WEBSITE expressly encouraged the sharing of videos between members. Language on that page reads "Post links with good photos and videos (preview is required!)."

In order to pass through the registration page and gain access to the actual content of the TARGET WEBSITE, a prospective user must create a "Nickname" and a password which must be entered along with a Captcha. A "Captcha" is a randomly generated series of characters designed to ensure that users of a website are human beings and not bots or other automated processes. Users are not required to enter any personally identifiable information, such as true names, emails or phone numbers. The users may also pick a color for their posts (or one was randomly generated) and click "enter chat."

Upon initially creating a user account on the TARGET WEBSITE, a user is assigned the status of "Guest." As an unregistered user, the user receives the following message upon log in: "You may check our rules by sending to me word rules. There also will be some additional explanation of how to use this feature. Do not reply this message. It is robot. News! We added features of forum. Access by button at the bottom or just by this link: forum. Unregistered users is able to write there too. Note that any content what you post less than 5yo or more than 13 yo will cause kick out of your retarted ass."

In order to fully register an account, the user would need to obtain a promotion from "Guest" to "Registered Guest," which is done at the discretion of TARGET WEBSITE staff. After an individual is promoted to a registered user account on the TARGET WEBSITE, a user must log in to that user account with the appropriate user-generated password in order to communicate via that user account on the TARGET WEBSITE. TARGET WEBSITE users may register, log into and access the TARGET WEBSITE through that user account using any computer or electronic device that is configured to use Tor routing/software. Unregistered or "Guest" users could access TARGET WEBSITE postings including postings that shared child pornography images.

As is common on these types of sites, the TARGET WEBSITE was administered and moderated by select TARGET WEBSITE users referred to as "Members" on this site. These users are promoted at the discretion of the site leadership. Promotions appeared to be made based on an individual's active participation on the site. Once promoted to a Member position, those users enforced the rules and assisted in the management of the site. This included controlling user membership using the "ban" and "kick" functions (which can limit or eliminate a user's participation or account), promoting within the ranks of users, and moderating the public chatroom for content and user behavior.

TARGET WEBSITE Members periodically re-posted standard messages to the public chatroom of the TARGET WEBSITE iterating rules and procedures of the TARGET WEBSITE. For example, on or about May 8, 2019, a Member posted "SECURITY INFORMATION" in the public chatroom. This post contained statements in both Russian and English which included but was not limited to the following:

- Set the Security Slider to HIGH Security Level

- Do Not Download if you are not using Encryption or Tails OS
- Read these manuals: → Tails Guide & Tor Security Guide ←

Do Not Share any Identifying Information & NEVER Trust Anybody!

Windows & OS X/MacOS are not safe for On topic[3]

Save files only to Encrypted Storage

Windows Leaves traces you cannot clean without a Full disk wipe

Linux offers Full Disk Encryption, Tails is Amnesic

use VeraCrypt to create Hidden Encrypted Containers

Open files when Offline to lower risk of malicious file causing trouble

LEA & Antis are known to pose as parents and kids to trick you into revealing information to them, suspect everyone is LEA.

LEA could be running this or any site at any time

Always be conscious your messages may not be private

Be Careful Paying for Anything, Bitcoin is not Anonymous by default!

The TARGET WEBSITE provides users with numerous links to image hosts where users can upload their digital images. For instance, on November 2, 2018, a TARGET WEBSITE user posted a hyperlink of a .jpeg file that linked to an image of a prepubescent boy being anally penetrated by an adult male's erect penis from behind. Also, on April 1, 2019, a TARGET WEBSITE user posted a hyperlink to a .jpg image depicting a nude prepubescent male sitting on a nude adult male's lap. The image only shows the males from the neck down. The adult male appears to be masturbating and is ejaculating or has ejaculated. The prepubescent male's erect penis is within inches of the adult male's erect penis. The adult male's right hand is around the

[3] Based on my training an experience, I am aware that "on topic" in this context refers to the advertisement, distribution and discussion of child pornography.

adult male's penis while his left hand is slid under the prepubescent male's buttocks. On May 29, 2019, a TARGET WEBSITE user posted a hyperlink to a .jpg image depicting a nude prepubescent boy standing next to a nude adult male. The prepubescent male has his hand around the nude adult male's erect penis while the prepubescent stares into the camera with an erection. The adult male is only visible from the neck down.

Postings to the TARGET WEBSITE that were publicly available to any registered user at the time of posting were captured and archived for law enforcement review. Over 1,400,000 messages were posted on the TARGET WEBSITE between March 2018 and July 2020. FBI Special Agents have accessed and downloaded child pornography files via links that were posted on TARGET WEBSITE, in an undercover capacity.

FLA described the website as facilitating "the sharing of child sexual abuse and exploitation material, stipulating only boys aged 5 – 13. Users were required to enter a username and password but these were only valid for that single login session" and provided further documentation naming the website as the TARGET WEBSITE, which the FLA referred to by its actual name.

16. In addition, postings to the TARGET WEBSITE that were publicly available to any registered user of the TARGET WEBSITE were captured and archived for law enforcement review. Review of such postings disclosed the following posts by TARGET WEBSITE users:

a. File "twlba5j7oo5g4kj5.onion (1).jpeg" depicts a naked prepubescent male, approximately four to six years old, sitting on a sofa and looking up at the camera. An erect, adult, penis is inserted in the mouth of the prepubescent male. (attached as Exhibit 1).

b. File "twlba5j7oo5g4kj5.onion (6).jpeg" depicts a naked prepubescent male, approximately seven to ten years old, kneeling between the legs of an adult male who is lying on

a bed. The erect penis of the adult male is inserted in the mouth of the prepubescent male. (attached as Exhibit 2).

c. File "twlba5j7oo5g4kj5.onion (7).jpeg" depicts a naked prepubescent male, approximately 4-6 years old, laying on a blanket on the floor. The prepubescent male is holding both legs, spread in the air, displaying his anus and genitals to the camera. (attached as Exhibit 3).

Evidence Related to Identification of Target that Accessed TARGET WEBSITE

17. I am aware that U.S. as well as foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the website(s) described herein. Those websites are globally accessible. The websites and their users may therefore be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the website is located or the offender appears to reside, in accordance with each country's laws.

18. In August 2019, a foreign law enforcement agency (referenced herein as "FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that FLA determined that on May 17, 2019, IP address 74.65.161.34 "was used to access online child sexual abuse and exploitation material" via a website that the FLA named and described as the TARGET WEBSITE.

19. FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

20. I am aware through my training and experience and consultation with other U.S. law enforcement agents that tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites have: (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

21. As described herein, the TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software on the user's computer could access the "TARGET WEBSITE." Even after connecting to the Tor network, however, a user would have to find the 16-or-56-character web address of the TARGET

WEBSITE in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16- or 56-character web address for a directory website in order to access it. While it operated, the web address for the website described herein was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

22. Accordingly, based on my training and experience and the information articulated herein, because accessing the TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

23. Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed the TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so.

Identification of SUBJECT PREMISES

24. According to publicly available information, IP address 74.65.161.34, which was used to access the TARGET WEBSITE on May 17, 2019, was registered to Charter Communications, Inc.

25. On November 19, 2019, a subpoena was issued to Charter Communications, Inc. in regard to the pertinent IP address. A review of the results obtained on December 26, 2019 identified the following account holder and address, which is the address of the SUBJECT PREMISES: Subscriber Name: Bradley Danforth; Subscriber Address: [redacted] Gardiner Maine 04345; Phone: 207-740-4472; Email Address: bdanforth1955@roadrunner.com.

26. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for Bradley Danforth. These public records indicated that Danforth's current address is [redacted], Gardiner, ME, the SUBJECT PREMISES. These checks also revealed that Danforth's spouse, Kendra Gero/Danforth (DOB in 1960), and an individual named Arnold Danforth (DOB in 1951) are also associated with the SUBJECT PREMESIS. Further checks on Kendra Gero/Danforth revealed that her car is registered at [redacted] in Gardiner, ME and her Maine driver's license lists her address as [redacted] in Gardiner, ME.

27. A check of the National Law Enforcement Telecommunications System (NLETS) on or about June 17, 2020 revealed that an individual named Bradley Danforth with a date of birth in 1955, has a valid Maine driver's license and resides at the SUBJECT PREMISES. NLETS and

CLEAR also reveal that Bradley Danforth has a Green 2001 Nissan Frontier with Maine license plate 6A8648 and a red 2007 Yamaha xv1700 motorcycle with Maine license plate 43EM registered in his name at the SUBJECT PREMISES.

28. A query of the National Crime Information Center (NCIC), through NLETS, conducted on or about June 20, 2020 determined that Bradley Danforth has no known criminal record.

29. A search of the CLEAR information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) for records associated with the Bradley Danforth was conducted on or about June 20, 2020, and the following information was revealed: Bradley Danforth purchased SUBJECT PREMISES on December 28, 2011. The deed transfer information states that SUBJECT PREMISES is a single-family residence-townhouse. The deed transfer information also states that Bradley Danforth is the sole owner of the SUBJECT PREMISES. CLEAR lists 207-740-4472 as a phone number for Bradley Danforth, which corroborates the information received in the November 19, 2019 subpoena to Charter Communications, Inc.

30. CLEAR also lists the SUBJECT PREMISES as the most recent address for Arnold Danforth, and shows that Arnold Danforth owns a Silver 2001 Oldsmobile Alero that is registered at the SUBJECT PREMISES. A check of NLETS for Arnold Danforth reveals that he has a Maine driver's license that expired on February 2, 2020, with the address of 14 Friendship Lane in Farmingdale, Maine. NLETS also confirmed that the Oldsmobile Alero is registered to Arnold Danforth at the SUBJECT PREMISES and has Maine license plate 3059SJ with an expiration date of April 30, 2021. A query of the NCIC, through NLETS, conducted on or about August 31, 2020 determined that Arnold Danforth had a Maine state arrest for public indecency in 1991, but that charge was dismissed after a court finding was filed.

30. Surveillance of the SUBJECT PREMISES on August 18, 2020 revealed that the residence is a grey one-story house with a grey roof and green trim. The house has an unattached garage located near the main residence. The SUBJECT PREMISES has two driveways, one that connects to Old Brunswick Road and one that connects to Brunswick Avenue, also known as Route 201.

31. On August 18, 2020, I used a smart phone wireless device in an effort to gain additional information regarding any potential wireless networks at the SUBJECT PREMISES. Positioned on the shoulder of Old Brunswick Road and then on the shoulder of Brunswick Avenue, directly in front of the SUBJECT PREMISES, I noted that there were multiple wireless networks in the area, but all of them were secured. Accordingly, to use any of them to access the Internet, a user would likely have to know the encryption key or password for that particular network. Based on the signal strength of the wireless networks, as well as my training and experience and information relayed to me by agents, I believe that the wireless router at the SUBJECT PREMISES is likely generating a secured wireless network. As explained above, I know, from my training and experience and information relayed to me by agents, that wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime.

32. A check of open source information from the Internet, such as Facebook and LinkedIn, regarding Bradley Danforth and Arnold Danforth revealed nothing.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

33. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage

devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored

in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

34. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[4]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers

[4] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as well as in his 2015 Jeep Compass, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

35. Based on all of the information contained herein, I believe that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access online child sexual abuse and exploitation material via a website. In particular, the target of investigation obtained and used Tor network software, found the web address for TARGET WEBSITE, and accessed online child sexual abuse and exploitation material via the TARGET WEBSITE.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

36. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

37. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

38. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of

their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs

may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the

criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

39. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is

essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

40. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter

an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

41. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

42. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

43. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Chase Ossinger
Special Agent
HSI

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedure

Date: Sep 08, 2020

City and state: Bangor, Maine

Judge's signature

John C Nivison U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

1. The entire property located at 2[redacted], Gardiner, ME, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). SUBJECT PREMISES is located on the North East side of Old Brunswick Road, seven houses on the left from the Brunswick Avenue intersection. The SUBJECT PREMISES is a grey one-story house with a grey roof and green trim. The house has an unattached garage located near the main residence. The SUBJECT PREMISES has two driveways, one that connects to Old Brunswick Road and one that connects to Brunswick Avenue, also known as Route 201. The SUBJECT PREMISES consist of the house, the unattached garage, and the vehicles registered to Bradley Danforth, namely a Green 2001 Nissan Frontier with Maine license plate 6A8648 and a red 2007 Yamaha XV1700 motorcycle with Maine license plate 43EM, and the vehicle registered to Arnold Danforth, namely a Silver 2001 Oldsmobile Alero with Maine license plate 3059SJ.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

   a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

   b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

   c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

   d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel Bradley Danforth to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the DEVICES found at the PREMISES, and

b. where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that Bradley Danforth state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES

Exhibit 14

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

District of New Hampshire

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
THE PREMISES KNOWN AS [redacted]UE, ROCHESTER, NH, AND ALL PE CLES ON PREMISES

Case No. 21-mj-146-01-AJ

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A(Attached and Incorporated Herein)

located in the _____ District of New Hampshire, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (Attached and Incorporated Herein)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252(a)(4)(B)	Illegal Possession of Child Pornography

The application is based on these facts:

See Affidavit (Attached and Incorporated Herein)

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Ronald Morin
Applicant's signature

Special Agent Ronald Morin, HSI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by **Telephonic conference** *(specify reliable electronic means)*.

Date: **Jun 4, 2021**

Andrea K. Johnstone
Judge's signature

City and state: Concord NH

Andrea K. Johnstone, United States Magistrate Judge
Printed name and title

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

District of New Hampshire

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
THE PREMISES KNOWN AS [redacted], ROCHESTER, NH, AND ALL PE ES ON PREMISES

Case No. 21-mj

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A(Attached and Incorporated Herein)

located in the _____ District of New Hampshire, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (Attached and Incorporated Herein)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252(a)(4)(B)	Illegal Possession of Child Pornography

The application is based on these facts:

See Affidavit (Attached and Incorporated Herein)

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Ronald Morin
Applicant's signature

Special Agent Ronald Morin, HSI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by **Telephonic conference** *(specify reliable electronic means)*.

Date: **Jun 4, 2021**

Judge's signature

City and state: Concord NH

Andrea K. Johnstone, United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AS [redacted], ROCHESTER NH AND ALL PEOPLE AND VEHICLES IN/ON THE PREMISES	)))))	**Case No. _____ FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Ronald Morin, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), being duly sworn, do depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing a search of the premises located at [redacted], Rochester NH ("SUBJECT PREMISES"), further described in Attachment A, to include all people and vehicles at the premises, and any computer, computer media, and electronic media located therein, for the things described in Attachment B—specifically, evidence, fruits, and instrumentalities of the foregoing criminal violations which relate to possession and access with intent to view child pornography.

2. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), and have been so employed since May 2006. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to child exploitation and child pornography. I have received training in the

area of child pornography and child exploitation, and as part of my duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

3. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The statements in this affidavit are based on my own investigation of this matter as well as on information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. While I have included all material facts relevant to the requested search warrant, I have not set forth all of my knowledge about this matter.

5. I submit that the facts set forth in this affidavit establish probable cause to believe that violations of 18 U.S.C. § 2252(a)(4)(B) have been committed and that there is probable cause to believe that fruits, evidence, and instrumentalities of the Specified Federal Offenses are likely to be found in the LAPTOP, as set forth below.

SPECIFIED FEDERAL OFFENSES

6. Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or

in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a) "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b) "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related toor operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

c) "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks,

external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

d) "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

e) "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

f) A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

g) "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network,

typically the Internet.

h) The "Darknet" is an overlay network within the Internet that can only be accessed with specific software, configurations, or authorization, and often uses a unique customized communication protocol.

i) The "Tor network" or "Tor" is free and open-source software for enabling anonymous communication by directing Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Tor is available to Internet users and is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit."

j) A "hidden service," also known as an "onion service," is website or other web service that is accessible only to users operating within the Tor anonymity network.

k) The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l) An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP

addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

m) "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n) "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

PROBABLE CAUSE

8. In February 2020, the HSI Manchester, NH, office received information that originated from a foreign law enforcement agency known to the Federal Bureau of Investigation (FBI) and with a history of providing reliable, accurate information in the past. In part, the information provided by the foreign law enforcement agency specified that on April 28, 2019, at 20:25:08 UTC, an individual originating from IP address 65.175.213.176 accessed a known Darknet web site that facilitated the sharing of child sex abuse and exploitation material with a particular emphasis on indecent material of young boys. Users of the website were able to view some material without creating an account. However, an account was required to post and access all content.

9. According to publicly available information, IP address 65.175.213.176 is owned

and operated by Atlantic Broadband. On or about September 9, 2019, a summons was served on Atlantic Broadband for subscriber information associated with the IP address on April 28, 2019 at 20:25:08 UTC. Atlantic Broadband provided the following subscriber details:

a. Subscriber name: Michael Clemence

b. Service and billing address: [redacted], Rochester NH

c. Phone numbers: 480-694-7209, 603-507-0703

10. A query of publicly available databases for information related to Michael Clemence revealed the following: year of birth 1985; last known address: [redacted], Rochester, NH ("The SUBJECT PREMISES"). The queries also indicated that Michael Clemence is married to Elizabeth Clemence and has two young children.

11. CLEAR records identified Michael Clements' date of birth as [REDACTED]/1985, SSN [REDACTED], address [redacted]. Rochester NH, email address enderwigman@msn.com. Criminal history checks revealed no derogatory information. Property record checks indicated that he purchased the SUBJECT PREMISES on 10/28/2019 with Elizabeth Anne Clemence.

12. On May 26, 2021, SA Mike Perella, Sean Serra, and Derek Dunn conducted a consensual knock and talk with Michael Clemence ("Clemence") at the SUBJECT PREMISES. Clemence answered the door and agents identified themselves. SA Perella advised Clemence that agents were at the SUBJECT PREMISES to ask about certain internet activity that occurred in April of 2019 at his previous residence, [redacted] in Rochester. Clemence expressed suspicion at the reason for agents' presence and advised that he had consumed a couple of beers. Clemence advised that his wife, Elizabeth, was at work.

13. During the conversation, Clemence volunteered that the tenant that lived next

door to him at [redacted] was an IT specialist and had done some IT work for him. Clemence identified this neighbor as "Kevin," and advised that he had since moved to Maine. Clemence was vague about the nature of the IT work Kevin had done for him in the past.

14. Agents advised Clemence that they were investigating internet activity associated with child exploitation material, and that some of this activity occurred in April 2019 from the IP address associated with his previous residence on Crow Hill Rd. Clemence expressed vague familiarity with the dark web, offering that he understood that it was used to buy and sell illegal drugs. When asked, Clemence denied any knowledge of Tor.

15. Clemence then described an event that took place around that same time in 2019 in which his wife was looking on their laptop and she viewed something that appeared to be "really bad." Clemence relayed that his wife was very alarmed at what she saw on the computer and she did not know what it was or how it got onto the computer. Clemence did not elaborate or provide specifics about what his wife had observed on the computer. After observing this material on the computer, he and his wife "wiped" the computer and gave it to a family friend.

16. Agents asked Clemence about the computer he currently had. In response, Clements stated that he had a computer that he used for work and offered to allow agents to conduct a manual review of this computer. A manual review was conducted onsite, and no illicit material was observed. Agents left their contact information with Clemence and advised that they would like Clemence's wife to contact them to arrange an interview. Clemence's wife, Elizabeth Clemence ("Elizabeth") contacted agents the following day and eventually made arrangements to be interviewed at her home on June 4, 2021.

17. On June 4, 2021 SA Mike Perella and I returned to the SUBJECT PREMISES at approximately 10:44 a.m. to conduct a consensual interview of Elizabeth Clemence. Elizabeth

disclosed that on May 18, 2019, she was printing church documents from a household computer and accessed a folder titled "Documents." She advised that the computer was a Dell laptop that belonged to her husband, but that they both used the computer. Within the "Documents" folder, she saw approximately 14,000 images and videos of what appeared to Elizabeth to depict child pornography. She described one file as two naked boys in a bathtub. In addition, Elizabeth advised that the filenames that she observed were consistent with child pornographic material. This occurred when they were living on Crow Hill Road in Rochester. Elizabeth advised that their internet connection at that home was secure and that nobody had the password.

18. When Elizabeth confronted Clemence about what she found on the computer, he stated he didn't know how it got there and suggested that their computer must have been hacked. Elizabeth explained that she and Clemence did not know what to do about what was on their computer. They considered going to the police, but at the time they were exploring the possibility of fostering children and they were concerned about jeopardizing their ability to do so. As a result, they decided to wipe the hard drive themselves. They also changed the passwords to the computer and the wireless internet. Elizabeth recalled it was possible that their neighbor, Kevin Mayfield, helped them change the password for the internet. They subsequently called an attorney the following Monday, and he concurred that it was good they wiped the hard drive. Elizabeth advised that she and Clemence were very concerned about the incident when it occurred and that they talked about it with their pastor and several close friends.

19. Elizabeth advised that at the beginning of the pandemic, a couple that they were friends with from church, Drew and Sarah Lytle, were in need of a computer for Zoom meetings. Elizabeth and Clemence decided to give them their Dell laptop computer. Prior to giving the computer to the Lytles, Elizabeth and Clemence wiped the hard drive a second time. The Lytles

gave the computer to their eldest son. Elizabeth advised that the Lytles live in Lebanon, Maine, and advised that after speaking with agents the week of May 26, 2021, Clemence did retrieve the Dell laptop computer from the Lytles.

20. Elizabeth advised that when she learned from Clemence that agents had been at their residence the previous week and learned the nature of their investigation, she checked all of the thumb drives in the house for the presence of child pornography. She advised that she did not locate any. Elizabeth further disclosed that she and Clemence have an "open marriage" in the sense that they share access to each other's online accounts, including email, social media, financial accounts, etc. They also share access to the electronic devices in the home.

21. Agents asked Elizabeth whose name the internet service was in at their previous address on Crow Hill Road. Elizabeth left the room to consult her records and returned with some paper files. Agents also inquired about who paid the bills, took care of household finances, etc., and Elizabeth stated that she did. Agents inquired whether she recalled any unusual or suspicious purchases around the time of April or May 2019 when this activity occurred. She indicated she could not recall anything offhand, but asked if she could consult her records. She left the room and returned with a laptop computer, which she used to access her financial accounts and did not find anything noteworthy.

22. Elizabeth asked whether there was anything else that she should "look for," and agents explained that they could not direct her to do any specific searching of Clemence's devices or accounts. However, they advised that there were certain applications and cloud storage accounts that are commonly encountered in these types of investigations. Elizabeth stated that Clemence did have a cloud storage account that she also had access to and stated that she was "on it right now." Agents advised Elizabeth that if she encountered anything concerning

in the accounts to which she and her husband shared access, she could contact them. Agents left their contact information and departed the SUBJECT PREMISES.

23. A short time later, while agents were en route back to their office, SA Morin received a telephone call from Elizabeth Clemence. Elizabeth disclosed that while reviewing the contents of Clemence's Google cloud account, she observed approximately four videos that appeared to depict child pornography. She described one such video as two male children that were clothed and spanking each other. Another video appeared to depict two young boys, approximately 13 years old, performing oral sex on each other. She later described a third video in which it appeared that an adult male was engaged in anal penetration of a prepubescent boy that appeared to be approximately 10 years old. The boy was blindfolded and had something over his mouth.

24. Elizabeth advised that the cloud storage account is connected to her husband's Gmail account, which is mike.clemence@gmail.com and that both the email address and password, both of which she has access to, are required to login to the Google cloud account. Elizabeth further stated that Clemence had access to his Gmail account on his cell phone.

25. Upon learning this information, agents determined that they would return to the SUBJECT PREMISES and secure it so that they could seek a search warrant. Agents arrived back at the residence at approximately 2:50 pm and observed a red Honda Civic with NH registration 3936669 parked in the driveway. Clemence was seated in the driver's seat with the driver's door ajar and one foot out the door. Clemence appeared to have his cell phone in his hand. When agents parked their vehicle, Clemence exited his car, leaving the door ajar, and placed his cell phone on the front passenger seat. SA Perella observed the cell phone in plain view on the vehicle seat and noticed that the screen was illuminated and it appeared that a video

was playing. SA Perella asked Clemence whether the cell phone on the seat was his, and Clemence confirmed that it was. SA Perella advised Clemence that agents would be securing the phone so that they could apply for a search warrant for its contents.

26. Clemence was extremely agitated and upset that agents had seized his phone. Agents explained that additional information had come to light since their interview with him the previous week. Agents explained that Clemence was not under arrest and that he was free to leave. Agents advised Clemence of his rights, and Clemence advised that he would like to speak with a lawyer. Agents offered the use of their own cell phones in order to allow Clemence to contact his attorney, but Clemence refused and insisted that he needed his own cell phone in order to get his attorney's contact information. Eventually, Clemence's wife provided a business card with their attorney's phone number on it, but Clemence still declined to use agents' phones to call his attorney. He left the SUBJECT PREMISES in his vehicle a short time later.

27. I reviewed two of the videos that Elizabeth previously described to me over the phone that appeared to Elizabeth to depict child pornography. Based on my training and experience, I agree that they appeared to depict child pornographic material. Elizabeth also described a concerning photograph of her 3 year old son that she found in the cloud storage account. She stated that her son was depicted naked from the waist down facing the wall. It appeared to have been taken in the home of the basement and depicted her son's buttocks. Elizabeth explained that Clemence is responsible for disciplining the children, and that when he does so he takes them to a private area of the house.

COMPUTERS, ELECTRONIC STORAGE

AND FORENSIC ANALYSIS

27. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives---contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

e. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

f. Your Affiant is aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize "cloud" storage. Cellular

telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

29. As set forth above, probable cause exists to believe that an individual at the SUBJECT PREMISES has distributed, transported, received, or possessed child pornography. Based upon my knowledge and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

a. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification.

b. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs,

correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

c. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

d. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; they conceal such correspondence as they do their sexually explicit material; and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

30. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such

as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be

sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it and when, it is sometimes necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

31. Based on my training and experience I know that much of the media referenced above, which may contain contraband, fruits and evidence of crime, is by its very nature portable. This includes as example but is not limited to extremely compact storage devices such as thumb drives, laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such media in multiple locations within their premises, including in outbuildings and motor vehicles, and/or on their person.

32. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the

storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. **The nature of evidence**. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

b. **The volume of evidence**. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files is evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. **Technical requirements**. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. **Variety of forms of electronic media**. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

33. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

34. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crime of possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) may be located at the SUBJECT

PREMISES. I therefore seek a warrant to search the SUBJECT PREMISES described in Attachment A and any computer and electronic media located therein, and to seize the items described in Attachment B.

35. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

/s/ Ronald Morin
Special Agent Ronald Morin
Department of Homeland Security
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Subscribed and sworn to before me on this 4th day of June, 2021.

Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

The premises to be searched includes:

1. The residential property located at [redacted], Rochester NH, including associated outbuildings and garages (the SUBJECT PREMISES);
2. Individuals and vehicles located on the premises; and
3. One black Samsung Galaxy S8+ cell phone, IMEI # 357725085185248, now in the custody of HSI Manchester, seized on June 4, 2021 from the vehicle of Michael Clemence while parked at the SUBJECT PREMISES.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252(a)(4)(B):

1. All records relating to violations of 18 U.S.C. §§ 2252(a)(4)(B) in any form wherever they may be stored or found at 31 Adams Avenue, Rochester, NH, including:

a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;

b. records or information pertaining to an interest in child pornography;

c. records or information pertaining to the possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

d. records or information of and relating to visual depictions that have been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256, including the record or information used to create the visual depiction;

e. records or information pertaining to Google;

f. photo-editing software and records or information relating to photo-editing software;

g. records or information relating to the occupancy or ownership of 31 Adams Avenue, Rochester, NH, including, but not limited to, utility and telephone bills, mail envelopes, vehicle registrations, tax bills, and other correspondence.

2. Any computer or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including possession and access with intent to view child pornography in violation of Title 18, United States Code, Sections 2252(a)(4)(B).

3. For any computer, computer hard drive, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

4. Records and things evidencing the use of the Internet, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term "COMPUTER" includes but is not limited to any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications

devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of New Hampshire

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
THE PREMISES KNOWN AS [redacted], ROCHESTER, NH, AND ALL PERSONS & VEHICLES ON PREMISES

Case No. 21-mj

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of New Hampshire
(identify the person or describe the property to be searched and give its location):
See attachment A (Attached and Incorporated Herein)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:
See Attachment B (Attached and Incorporated Herein)

YOU ARE COMMANDED to execute this warrant on or before June 18, 2021 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Andrea K. Johnstone, United States Magistrate Judge.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 8:17 PM, Jun 4, 2021

Andrea K. Johnstone
Judge's signature

City and state: Concord NH

Andrea K. Johnstone, United States Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.: 21-mj	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AS [redacted], ROCHESTER NH AND ALL PEOPLE AND VEHICLES IN/ON THE PREMISES	)	**Case No. _____** **FILED UNDER SEAL**

MOTION TO SEAL AT LEVEL I: ENITRE MATTER
RELATED TO APPLICATION FOR SEARCH WARRANT

In the above captioned case, the United States of America respectfully moves to seal at Level II the entire matter related to the Application for a Search Warrant, including the application, the supporting affidavit, any search warrant that may issue, the resulting return, this motion, and the corresponding docket text entries for **90** days, expiring on **June 28, 2021.**

Under Federal Rule of Criminal Procedure 49.1(d) and Local Rule 83.12(a)(1), the Court has authority to grant this motion.

The Court should seal these documents because they contain sensitive information, which, if prematurely released, may compromise an ongoing criminal investigation. Specifically, the supporting affidavit contains information identifying potential targets of the investigation. Investigators believe that those targets are unaware that they are considered suspects or are unaware of the incriminating evidence investigators have gathered against them. Should information identifying those targets and the evidence against them be released, it may cause them to flee, destroy evidence, or change their patterns of behavior.

This motion is not intended to preclude the executing officer from serving a copy of the warrant and a receipt for any property seized as required by Federal Rule of Criminal Procedure 41(f)(1)(C).

Respectfully submitted,

JOHN J. FARLEY
Acting United States Attorney

Dated: June 4, 2021

By: /s/ Kasey Weiland
Kasey Weiland
Assistant United States Attorney
United States Attorney's Office
53 Pleasant Street, 4th Floor
Concord, NH 03301
(603) 225-1552
kasey.weiland2@usdoj.gov

Motion: ☑ Granted ☐ Denied

Andrea K. Johnstone
United States Magistrate Judge
United States District Court
District of New Hampshire
Date: **Jun 4, 2021**

Exhibit 15

CONTINUATION IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Scott Robinson, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the FBI since 2019 and am currently assigned to the Detroit Division. My duties include the investigation of alleged violations of federal criminal laws, including the subject offense, sexual exploitation of children (18 U.S.C. §§ 2251 and 2252A).

2. This continuation is submitted in support of an application, under Rule 41 of the Federal Rules of Criminal Procedure, for a search warrant for the locations specifically described in Attachment A, including the entire property located at [redacted], **Lansing, Michigan 48912** (the "SUBJECT PREMISES") and the content of electronic storage devices located therein, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (access with intent to view child pornography), which items are more specifically described in Attachment B.

3. The statements contained in this continuation are based in part on information provided by U.S. federal law enforcement agents, written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information

gathered from investigative sources of information, and my experience, training and background as a Special Agent.

4. This continuation is submitted for the limited purpose of securing a search warrant. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of federal law are located at the SUBJECT PREMISES.

SUMMARY OF INVESTIGATION

5. A user of the internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography. The child pornography is housed on a website operated on the Tor anonymity network.

I. The Tor Network

6. The internet is a global network of computers and other devices. Devices directly connected to the internet are uniquely identified by IP addresses. IP addresses are used to route information between internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address. This way, the responding device knows where to send its response. On the internet, data transferred between devices is split into discrete packets, each of which has two parts: (1) a header with non-content routing and control information, such as the packet's source and destination IP addresses;

and (2) a payload, which generally contains user data or the content of a communication.

7. TARGET WEBSITE operated on the Tor network. The Tor network is a computer network, available to internet users, that is designed specifically to facilitate anonymous communication over the internet. The Tor network routes communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional techniques to identify a user's IP address are not effective.

8. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website. The Tor browser is a web browser that is configured to route a user's internet traffic through the Tor network.

9. As with other internet communications, a Tor user's communications are split into packets containing header information and a payload, and those communications are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next

node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

10. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses an internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. The encryption prevents the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

11. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

12. The Tor Network also makes it possible for users to operate websites, such as those described herein, called "hidden services" or "onion services," in a

manner that attempts to conceal the true IP address of the computer hosting the website. Hidden service websites are accessible only to users operating within the Tor network. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

13. Unlike standard internet websites, a Tor-based web address is comprised of a series of at least 16 and as many as 56 algorithm-generated characters, for example "asdlk8fs9dflku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. There is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. While law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

II. Description of TARGET WEBSITE

14. The conduct being investigated involves users of a Tor-network-based website; TARGET WEBSITE. The TARGET WEBSITE was an online bulletin board dedicated to the advertisement and distribution of child pornography that operated from approximately at least September 2016 to June 2019. In June of 2019, the computer server hosting the TARGET WEBSITE, which was located outside of the United States, was seized by a foreign law enforcement agency.

15. A review of the initial TARGET WEBSITE page revealed it was a message board web page that contained a search bar, and showcased two hyperlinks titled, "Announcements" and "Important Information." Located below the title were hyperlinks including those entitled "Quick Links," "Home," "Board Index," "Login," and "Register." As of June 2019, the website had over 820,000 members and over 81,000 postings.

16. Upon accessing the "Announcements" hyperlink of the TARGET WEBSITE, the following message was displayed in message board form, "Welcome, Please read before registering" which was dated July 1, 2016. Upon accessing the aforementioned hyperlink, the message read, "Welcome abusers and abusees and those that enjoy watching. This website was created to host videos, photos and discussions of 18 (twinks) and younger of Hurtcore materials (videos & pictures) as well as discussion of such." Based on my training and experience, I know that

Hurtcore refers to violent pornography. The message continued, "PS Please register to see all the forums, and use strong password for user profile."

17. Upon accessing the "Register" link of the TARGET WEBSITE, it was revealed that users would complete a "Username," "Password," "Confirm password," "Language," and "My timezone," fields, as well as a "Confirmation of Registration" code. Upon entering the TARGET WEBSITE, sections and forums for posting to the website included "HURTCORE Toddlers Videos (Ages 0-5)," "Preteen/Hebe Children Videos (Ages 6-13)," "Teens Videos (Ages 14+)," "Toddlers Images (Ages 0-5)," "Preteen/Hebe Children Images (Ages 6-13)," and "Teens Images (Ages 14+)." Based on my training and experience, I know that "Hebe" is a reference to a "hebephile," which is a person with a persistent sexual interest in pubescent minor children. Another forum was named "GORE/DEATH" which included sub-forms for "Toddlers (Ages 0-5)," "Preteen/Hebe Children (Ages 6-13)" and "Teens (Ages 14+)." An additional section of the website called "The Team" listed the usernames of two website "Administrators" and five "Global Moderators." The TARGET WEBSITE also contained a private message feature that was available, allowing users to send private messages to each other.

18. On June 23, 2016, a website administrator posted a topic entitled "Board Rules" in the "Important Information" forum which contained the following explanation of the website:

> Rules are simple all material must be related to Hurtcore content. What is Hurtcore content? It is rape, fighting, wrestling, bondage, spanking,

> pain, mutilation, gore, dead bodies, and etc. (no limits) Why does this place exist? There was a need and since society thinks I am worst than any abuser or creator of Hurtcore content, I decided to create this place for those who like it and want to share. Besides I am the mischievous god. It is up to you to make this the best Hurtcore board there is. So please upload whatever you can so that it can be shared.

19. A review of the "Toddlers Videos," "Preteen/Hebe Children," "Toddlers Images," and "Gore/Death" forums and subforums, as well as additional forums, within the various above sections revealed they contained numerous pages of topics. Each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the thread below it. Typical posts appeared to contain text, images, thumbnail previews of images, links to external sites with compressed files (such as ".rar"), or replies to previous posts.

20. A review of topics within these sections revealed numerous posts containing images and/or videos depicting child pornography and child erotica of prepubescent males, females, toddlers, and infants; including those depicting anal, vaginal, and oral penetration. Additionally, these sections revealed numerous posts containing images and/or videos depicting child pornography involving gore and sometimes death. Examples of these are as follows:

a. On October 9, 2016, a website user posted a topic entitled "Fuck the newborn. Real fuck!" in the "Hurtcore/Toddlers Images/Girls" forum, that contained nine

images depicting child pornography and child erotica of a prepubescent female infant. One of these images depicted a naked female infant lying on her back with her legs spread apart, exposing her vagina, with a gloved adult finger inserted into her anus. A male's penis was pressed against her vagina and the head of the penis inserted into her mouth. A brown liquid substance, appearing to be the infant's feces are seen smeared around her anus.

b. On November 5, 2016, a website user posted a topic entitled "BabyHee 1yo (one of full version)" in the "HurtCore/Toddlers Videos/Boys" forum that contained images depicting child pornography and torture of a prepubescent male, who was completely naked and tied down with rope on the side of a bath tub. Among other things, the images depicted an adult male defecating on the chest and urinating in the mouth of the prepubescent male.

III. Hidden Service Websites and TARGET WEBSITE

21. As described herein, TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software could access TARGET WEBSITE. Even after connecting to the Tor network, a user would have to find the 16-character web address of TARGET WEBSITE in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—like websites that operate on the open internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open internet websites for a particular

content of interest. Users interested in accessing child exploitive material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitative related content. Those directory sites also operate via the Tor network.

22. Users utilize directory sites to identify new web forums, chat sites, image galleries, and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are operating, whether images of child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory site in order to access it. While it operated, the web address for TARGET WEBSITE was listed on one or more of these directory sites advertising hidden services dedicated to the sexual exploitation of children.

23. Based on my training and experience, because accessing TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

24. Based on my training and experience, I know that it is extremely rare for an individual who takes the numerous positive steps to find child pornography on a Tor hidden services website to only visit that website one time. One example of this is analysis of "Playpen", which was a Tor network-based hidden service dedicated to the advertisement and distribution of child pornography that operated from August 2014 until March 2015. Similar to TARGET WEBSITE, Playpen was a highly categorized web forum with hundreds of thousands of users. It allowed users to post and download messages pertaining to child exploitation within forum categories. The categories were indexed by the age and gender of child victims and the type of sexual activity involved. In February and March of 2015, the FBI seized and briefly operated the Playpen website for two weeks, using a court-authorized investigative technique to successfully identify IP addresses and other information associated with site users. The FBI's review of site data seized from the Playpen website during the operation determined that, of over 400,000 total user accounts observed on the Playpen website during its existence, less than 0.02 percent (that is, less than two hundredths of one percent) of user accounts with a registered account on the website accessed a message thread on the website only once.

25. Probable cause exists that any user who accessed TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so.

26. U.S. and foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as TARGET WEBSITE and other websites described herein. Those websites are globally accessible. The websites and their users may be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, in accordance with each country's laws, it is common practice for that law enforcement agency to share information with law enforcement (1) in the country where the site is located; or (2) where the offender appears to reside.

27. In August of 2019, a Foreign Law Enforcement Agency (referenced herein as "FLA") known to the FBI, and with a history of providing reliable, accurate information in the past, contacted the FBI. The FLA provided the following information:

28. On May 14, 2019, at 19:52:14 UTC[1], a user of IP address 52.144.38.57 accessed online child sexually abusive and exploitive material via a website on the Tor network, the TARGET WEBSITE;

[1] UTC is Coordinated Universal Time; it is five hours ahead of Eastern Standard Time.

a. The website was described as having *"an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children,"*;

b. *"[u]sers were required to create an account (username and password) in order to access the majority of the material,"*; and

c. documentation naming TARGET WEBSITE, which the FLA referred to by its actual name.

29. According to publicly available information, IP address 52.144.38.57 was registered to Lightspeed Communications.

30. On January 3, 2020, through a subpoena, the FBI determined that Lightspeed Communications IP address 52.144.38.57 resolved to Nicole Hope, [redacted], **Lansing, Michigan 48912**, which is the address of the SUBJECT PREMISES.

31. A search of a public records database for the SUBJECT PREMISES revealed that, since approximately 2018, Nicole Hope, date of birth [redacted], 1983, is likely the current resident. Daniel Conlin Jr., date of birth [redacted],1987, is also a likely resident. Records from the Michigan Secretary of State showed that Nicole Hope and Daniel Conlin Jr. have driver's licenses that list the home addresses as the SUBJECT PREMISES.

32. On August 3, 2020, the U.S. District Court for the Western District of Michigan authorized the installation and use of a pen register/trap and trace device (PRTT) to record, decode and/or capture all dialing, routing addressing and signaling information associated with each communication to or from the residential internet service account associated with the SUBJECT PREMISES provided by Lightspeed Communications. A renewal of the PRTT was authorized on September 17, 2020.

a. Based on my training and experience, I am aware that analysis of data obtained via a PRTT on a target's residential internet connection can provide evidence that a user of the internet at the premises is accessing the Tor network. That is possible because the IP addresses of Tor node computers that make up the network are published by the Tor network. Since a residential internet PRTT will disclose the IP addresses of computers to which communications are sent and from which communications are received, analysis of the PRTT data can reveal Tor use. Due to Tor routing and encryption, a PRTT will not reveal the ultimate destination or the content of those communications.

b. Lightspeed Communications began to provide data for this PRTT on September 15, 2020. Analysis through November 16, 2020 of the data provided pursuant to that PRTT order revealed evidence that a user of the internet at the SUBJECT PREMISES accessed the Tor network on eight separate days since Lightspeed Communications started providing data:

i. September 16, 2020 at 6:49 a.m.;

ii. September 26, 2020 at 11:04 p.m.

iii. October 31, 2020 at 1:09 p.m.

iv. November 9, 2020 at 11:25 p.m.

v. November 10, 2020 at 1:05 p.m.

vi. November 12, 2020 at 1:22 p.m. and 2:33 p.m.

vii. November 13, 2020 at 5:58 p.m.

viii. November 15, 2020 at 11:44 a.m., 1:16 p.m., and 1:58 p.m.[2]

33. Based on my training and experience, although the TARGET WEBSITE is no longer in service, the fact that an internet user at the SUBJECT PREMISES continue to access the Tor network means that it is likely the user is continuing to use the Tor network for child exploitation purposes. While I know that the Tor network contains sites other than those involving child pornography, I know based on my training and experience that the Tor network contains many sites dedicated to child pornography and child exploitation, just like the TARGET WEBSITE, and individuals that seek out child pornography will continue to do so even if a website they have utilized in the past is no longer in service.

[2] All times listed in this paragraph are in Eastern Standard Time.

IV. The Foreign Law Enforcement Agency

34. The FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of reciprocal criminal investigative cooperation between U.S. law enforcement and the FLA. This cooperation includes the investigation of crimes against children. The FLA advised U.S. law enforcement that it obtained the information through an independent investigation that was lawfully authorized in the FLA's country pursuant to its national laws. Further, the FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain the 52.144.38.57 IP address information. U.S. law enforcement personnel did not participate in the investigative work through which the FLA identified the 52.144.38.57 IP address provided by the FLA.

35. I am aware through my training and experience, and through consultation with other U.S. law enforcement agents, that tips provided by the FLA, regarding IP addresses that the FLA advised were associated with access to Tor network child exploitation-related web and chat sites, have: (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to

be related to targets that U.S. law enforcement investigations had independently determined were associated with the trafficking and possession of child pornography.

Background on Child Pornography, Computers, and the Internet

36. Based on my training, experience, and information obtained from other agents, I know the below statements are accurate.

37. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

38. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as WiFi or Bluetooth. Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

39. Any computer can connect to any smartphone, tablet, or other computer. Through the internet, electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

40. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

41. The internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

42. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the internet. Even in cases where online storage is used, however, evidence

of child pornography can be found on the user's computer, smartphone, or external media in most cases.

43. Individuals commonly use smartphone and computer apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

44. Communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Specifics Related to the Search and Seizure of Computer Systems

45. As described above and in Attachment B, this application seeks permission to search for evidence that exists in the SUBJECT PREMISES, in whatever form they are found. The evidence is likely to be found on and stored in a computer's hard drive or other storage media. Thus, the warrant applied for would

authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

46. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe the evidence referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file;

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic

evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information; and

d. Files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

47. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. Probable cause exists that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES.

48. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can

reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

49. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media.

50. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers

typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

51. Some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data also typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user.

52. Information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the

computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

53. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

54. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

55. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

56. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an

instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used, data that was sent or received, notes as to how the criminal conduct was achieved, records of internet discussions about the crime, and other records that indicate the nature of the offense.

57. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises, it is not always possible to search computer equipment and storage devices for data for a number of reasons.

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search

site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension

".jpg" often are image files. A user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text.

e. Computer users can also attempt to conceal data by using encryption. Encryption involves the use of a password or device, such as a "dongle" or "keycard," to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

f. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (an individual may access the wireless network without a key or password) wireless routers for both networks may yield

significant evidence of, or serve as instrumentalities of, a crime. This includes identifying the instrument through which the perpetrator of the internet-based crime connected to the internet. This may potentially contain logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

58. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium. This might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Request to Use Biometric Data to Unlock Devices

59. This warrant seeks to permit law enforcement to compel all residents of the SUBJECT PREMISES who are present at the SUBJECT PREMISES to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called

"Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

60. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are

considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

61. As discussed, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant are currently unknown to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

62. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features,

the opportunity to unlock the device through a biometric feature may exist for only a short time.

63. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of all residents of the SUBJECT PREMISES who are present at the SUBJECT PREMISES to the fingerprint scanner of the DEVICES found at the SUBJECT PREMISES; (2) hold the DEVICES found at the SUBJECT PREMISES in front of the face of all residents of the SUBJECT PREMISES who are present at the SUBJECT PREMISES and activate the facial recognition feature; and/or (3) hold the DEVICES found at the SUBJECT PREMISES in front of the face of all residents of the SUBJECT PREMISES who are present at the SUBJECT PREMISES and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that all individuals present at the SUBJECT PREMISES to state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel all individuals present at the SUBJECT PREMISES to identify the specific biometric characteristics (including the unique

finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

64. For the foregoing reasons, I submit that probable cause exists that contraband, property, evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (access with intent to view child pornography), more fully described in Attachment B, will be located at the locations described in Attachment A.

Exhibit 17

b7E -5

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 01/24/2017

Preliminary investigation of a TOR Hidden Service known as [redacted] was conducted by SA [redacted]

b6 -1
b7A -1
b7C -1
b7E -4,5

[redacted]

b7A -1
b7E -4,5

[redacted]

b7A -1
b7E -4,5

[redacted] 18 (twinks) and younger [redacted]

[redacted]

b7A -1
b7E -4,5

[redacted]

b7A -1
b7E -4,5

[redacted]

b7A -1
b7E -4,5

[redacted]

b7A -1
b7E -4,5

[redacted]

b7A -1
b7E -4,5

Investigation on 01/13/2017 at [redacted] United States (In Person)

b6 -1
b7C -1
b7E -5

File # [redacted] Date drafted 01/17/2017

by [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Exhibit 39

Operation H

focused on stopping the spread of some of the most egregious and devastating examples of child exploitation material found on the internet to date. It is the largest operation of this kind, led out of New Zealand. It brought together national and international agencies including NZ Police, Customs, Europol, INTERPOL and the 5 Eyes.

Te Tari Taiwhenua
Internal Affairs

Key Statistics

Statistics correct as of 01/03/2022

Worldwide

13
Countries

17
Agencies

836
Cases investigated

146
Children safeguarded

New Zealand

The Department of Internal Affairs, along side NZ Police and Customs swiftly identified perpetrators, issued warrants and prosecuted New Zealand individuals that downloaded and spread the material.

71
Suspects identified

46
Arrested

12
Investigation in progress

6
Children safeguarded

Internationally

New Zealand worked with multiple countries and agencies including our large international partners.

Region	Cases investigated	Children safeguarded
New Zealand	71	6
Europe	72	1
United Kingdom	450	79
Canada	47	12
Australia	156	44
Singapore	4	-
United States of America	36	4

What happened

We acted quickly to identify key material, work with our partner agencies to quickly arrest perpetrators.

Sep2019
Investigation commenced after receiving a report from an Electronic service Provider (ESP).

Oct2019
ESP uncovered over 90K users of child exploitation material and DIA undertook extensive analysis of account information.

Oct- Nov 2019
Government analysis completed Domestic agencies begin their own investigations.

Nov 2019 - Feb 2020
Operational planning commences New Zealand continued to extensively assist our international partners for their investigations.

Feb 2020 onwards
Government undertook warrants and prosecutions DIA and NZ Police, along with intelligence assistance from NZ Customs Service, begin issuing warrants and prosecutions

NEW ZEALAND POLICE Ngā Pirihimana o Aotearoa
NEW ZEALAND CUSTOMS SERVICE TE MANA ĀRAI O AOTEAROA
EUROPOL
NCA National Crime Agency
AFP AUSTRALIAN FEDERAL POLICE
INTERPOL

Operation H

focused on stopping the spread of some of the most egregious and devastating examples of child exploitation material found on the internet to date. It is the largest operation of this kind, led out of New Zealand. It brought together national and international agencies including NZ Police, Customs, Europol, INTERPOL and the 5 Eyes.

Te Tari Taiwhenua
Internal Affairs

Internationally

Statistics correct as of 01/03/2022

Country	Region	Cases investigated	Children safeguarded
New Zealand	N/A	71	6
Czech Republic	N/A	8	-
Croatia	N/A	19	-
Greece	N/A	3	-
Hungary	N/A	30	1
Slovenia	N/A	8	-
Spain	N/A	2	-
Slovakia	N/A	2	-
United Kingdom	N/A	450	79
Canada	Prince Edward Island	2	-
	Ontario	26	3
	Nova Scotia	3	-
	Manitoba	2	-
	Saskatchewan	1	-
	Alberta	3	-
	British Columbia	3	7
	Quebec	7	2
Australia	Northern Territory	2	-
	New South Wales	26	3
	Victoria	27	8
	Australian Capital Territory	5	5
	Tasmania	4	2
	Queensland	69	16
	Western Australia	8	-
	South Australia	15	10
Singapore	N/A	4	-
United States of America	N/A	36	4

NEW ZEALAND POLICE Ngā Pirihimana o Aotearoa
NEW ZEALAND CUSTOMS SERVICE TE MANA ĀRAI O AOTEAROA
EUROPOL
NCA National Crime Agency
AFP AUSTRALIAN FEDERAL POLICE
INTERPOL

JA 1234

Operation H

focused on stopping the spread of some of the most egregious and devastating examples of child exploitation material found on the internet to date. It is the largest operation of this kind, led out of New Zealand. It brought together national and international agencies including NZ Police, Customs, Europol, INTERPOL and the 5 Eyes.

Te Tari Taiwhenua
Internal Affairs

Countries that INTERPOL has engaged with

Countries correct as of 01/03/2022



JA1235

Exhibit 41

INTERPOL

INTERPOL supports New Zealand-led international operation into online child sexual abuse material

2 March 2022

146 children safeguarded internationally

LYON, France – An international operation led by New Zealand's Te Tari Taiwhenua Department of Internal Affairs (DIA) has identified more than 90,000 online accounts that have possessed or traded child sexual abuse material.

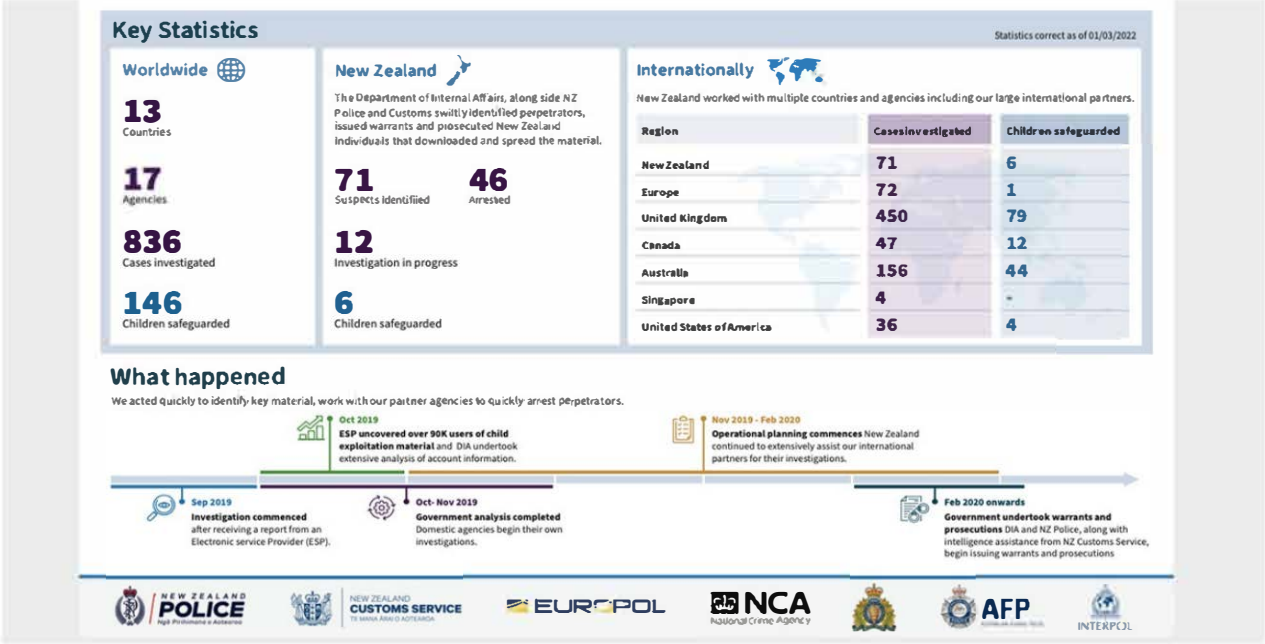
In what officials have called 'the largest and most challenging online child exploitation operation led out of New Zealand', the DIA brought together international law enforcement agencies, including INTERPOL, to assist and coordinate what became hundreds of investigations across the world.

The Operation, Codenamed 'H', was launched in October 2019 by DIA's Digital Child Exploitation Team following an alert from an Electronic Service Provider who had found tens of thousands of offenders using the platform to share some of the most horrific and devastating child sexual abuse material online.

The two-year long operation has produced the following results:

- 46 New Zealand based individuals arrested
- 836 cases investigated internationally
- 146 children safeguarded internationally

Our site uses cookies to ensure technical functionality, gather statistics and enable sharing on social media platforms. Tell me more



Tim Houston, Manager Digital Child Exploitation Team and lead for Operation H, highlighted how this operation and the prosecutions that will follow represent a major success in international efforts to undermine and disestablish the environments and networks that seek to exploit children.

“I commend the ongoing support of our law enforcement partners domestically and across the world for their dedication and hard-work. This operation will have an impact on the global networks that deal in the most horrific and damaging material, and we are extraordinarily proud of the effect it will have on children’s lives around the world,” said Mr Houston.

To support New Zealand’s efforts and ensure a global net was cast, INTERPOL’s Crimes Against Children (CAC) unit disseminated referral packages to 130 countries, concerning approximately 153,000 accounts. The unit then actively engaged with 58 member countries to provide them with the child abuse material relevant to subjects in their jurisdiction, as well as related intelligence.

INTERPOL’s Crimes Against Children (CAC) unit disseminated referral packages to 130 countries, concerning approximately 153,000 accounts.

The referral process has afforded the opportunity for many INTERPOL member countries to exercise and

Our site uses cookies to ensure technical functionality, gather statistics and enable sharing on social media platforms. Tell me more

Additionally, a selection of images and videos was uploaded to INTERPOL's International Child Sexual Exploitation (ICSE) database, contributing to further investigations aimed at identifying victims and offenders. The database currently includes material and information relating to more than 27,700 identified victims and some 12,500 offenders worldwide, as well as images and videos depicting the abuse of victims yet to be safeguarded.

COUNTRIES INVOLVED

NEW ZEALAND

RELATED DOCUMENTS

Operation H in numbers 1.73MB • EN

SEE ALSO

Crimes against children

International Child Sexual Exploitation database

Related news

Our site uses cookies to ensure technical functionality, gather statistics and enable sharing on social media platforms. Tell me more



abuse in the aid sector

17 February 2022



INTERPOL General Assembly resolution calls for increased safeguards against online child sexual exploitation

24 November 2021



Ground-breaking insights into the risk of online child sexual exploitation and abuse in Kenya

27 October 2021



Expand use of INTERPOL to address global crime threats - G7 Ministers

10 September 2021

Our site uses cookies to ensure technical functionality, gather statistics and enable sharing on social media platforms.

Tell me more

Exhibit 42

News

450 users of child abuse platform arrested in the UK

Child sexual abuse (/component/tags/tag/child-sexual-abuse)

450 people have been arrested in the UK after they were identified as members of an online platform used for trading child sexual abuse material.

The material was some of the most 'horrific and devastating' investigators had seen. It included a particularly disturbing and sadistic video series, which showed the torture, rape and sexual abuse of three kidnapped young girls, one of whom was an 18 month old toddler.

Authorities in New Zealand, where the platform was hosted, launched an investigation in October 2019 and identified tens of thousands of global users.

Information relating to accounts believed to have been created in the UK was passed to the National Crime Agency. The NCA launched a high priority operation to analyse the data, before initiating its own investigations, as well as disseminating packages to law enforcement partners across the country.

So far, 450 UK-based users of the platform have been arrested by police, Regional Organised Crime Units (ROCUs) and the NCA, for a variety of child sexual abuse offences.

NCA investigations alone have led to the arrest of 95 people, with 42 having been charged to date and 28 convicted. NCA officers have also safeguarded 79 children.

Although many were initially arrested for their roles in sharing child abuse material on the platform, this often led investigators to uncover further serious offending, including contact abuse.

NCA officers arrested Robert Stanley from Essex in April 2020 after receiving intelligence he had accessed three Category A (the most serious) child abuse videos. Analysis of his phone uncovered screenshots of a video call with his partner, Danielle Schofield of West Yorkshire, where she sexually abused an eight-year-old girl. Messages also showed the pair fantasising about kidnapping, gagging and keeping a child chained up as their 'sex slave'. They were jailed for a total of seven years and nine months in April 2021.

Quick exit (https://ww

In August last year, Steven Skelton from Folkestone was jailed for ten years, after a Kent Police investigation found he had been directing the abuse of hundreds of children around the world. He had in his possession more than 230 videos showing victims as young as seven live streaming themselves between 2019 and 2020. On one of his phones was a conversation in which he sent sexual messages to a 13-year-old girl, who officers identified and safeguarded.

Many of the UK offenders were also working in positions of trust, including at primary schools and nurseries, within law enforcement, as medical professionals, and some as religious officials.

Other suspects were in the process of applying for jobs working or volunteering with children.

In May 2020, NCA officers arrested brothers Akaash and Nadeem Hussain, from Sheffield, after the pair were found to have signed up to the platform. Akaash, a night support worker at a children's home, had 200 indecent images of children (IIOC) on his phone. Nadeem had downloaded over 400 and both pleaded guilty to making IIOC.

Sarah Blight, Deputy Director of the Child Sexual Abuse Threat at the National Crime Agency, said: "This has, and continues to be, a hugely important operation. The information received from our partners in New Zealand pointed to a significant number of online accounts linked to individuals in the UK, who likely pose a sexual threat to children.

"After analysing this data, we were able to prioritise those offenders believed to pose the highest risk, and share details with our policing partners throughout the UK. This has so far led to the arrest of 450 suspects, some of whom were already known to law enforcement and many of whom were working in positions of trust.

"Much of this activity took place during the Covid-19 lockdowns, when the majority of young people were at home and offenders had more time to spend online targeting their victims. Identifying and safeguarding vulnerable children during this period was our absolute priority.

"Work is very much ongoing across the country to disrupt more of these sexual predators. Each month the NCA and UK policing arrest around 850 suspects and safeguard over 1,050 children. The NCA is focusing on the most dangerous offenders; we have the specialist capabilities to

identify them and ensure they are brought to justice."

01 March 2022

Latest from twitter

Quick exit (https://ww

National Crime Agency (NCA)
@NCA_UK

Replying to @NCA_UK

The NCA is able to use tools such as civil recovery orders, to ensure those who benefit from the proceeds of crime do not hold on to illicit wealth.

These assets will eventually be sold with the proceeds going towards combatting further crime.

9h

National Crime Agency (NCA)
@NCA_UK

Replying to @NCA_UK

Those properties were collectively valued at £1.08 million and eventually became the subject of the NCA's civil recovery claim in 2019.

Approximately £650,000 of the property value is believed to have originated from the mortgage fraud.

9h

National Crime Agency (NCA)
@NCA_UK

Replying to @NCA_UK

Officers identified the proceeds of a mortgage fraud, totalling almost £420K into the Route of Asia account.

In 2009 Miah used almost £300K of this money towards buying the Warwick Arms. He sold the business five years later and used the proceeds to buy another four properties.

9h

National Crime Agency (NCA)
@NCA_UK

Replying to @NCA_UK

@leicspolice began investigating in 2009, after it became aware of funds being paid through a money service business account called 'Route of Asia', leading them to suspect the owner, Salim Miah, of operating a large scale money laundering scheme.

Quick exit (https://ww

Share this page:

TOP ^

0370 496 7622

NCA general enquiries or to verify an NCA officer, available 24/7

CLICK CEOP Advice Help Report

(https://www.ceop.police.uk)

Who we are (/who-we-are)

Our mission (/who-we-are/our-mission)

What we do (/what-we-do)

How we investigate (/what-we-do/crime-threats)

How we work (/what-we-do/how-we-work)

News (/news)

Most wanted (/most-wanted-search)

Careers (/careers)

A day in the life (/careers/a-day-in-the-life)

Current vacancies (/careers/vacancies)

Contact us (/contact-us)

Operation Stovewood (/what-we-do/crime-threats/operation-stovewood-rotherham-child-sexual-abuse-investigation)

Suspicious activity reports (https://www.ukciu.gov.uk/saronline.aspx)

Verify an NCA officer (/contact-us/verify-an-nca-officer)

Complaints (/contact-us/complaints)

Follow us

(https://www.facebook.com/nationalcrimeagency/) (https://twitter.com/NCA_UK) (https://www.instagram.com/nationalcrimeagency/) (https://www.linkedin.com/company/national-crime-agency)

Quick exit (https://ww

© Crown Copyright

Exhibit 43

The Department of Internal Affairs

Te Tari Taiwhenua | Department of Internal Affairs

Building a safe, prosperous and respected nation

New Zealand led international operation into online child sexual abuse material leads to 46 arrests across New Zealand

2 March 2022

An international operation led by Te Tari Taiwhenua Department of Internal Affairs (DIA) has identified more than 90,000 online accounts that have possessed or traded child sexual abuse material.

Operation H was launched in October 2019 by DIA's Digital Child Exploitation Team following an alert from an Electronic Service Provider who had found tens of thousands of offenders using the platform to share some of the most horrific and devastating child sexual abuse material online.

This has been the largest and most challenging online child exploitation operation led out of New Zealand.

To carry out this Operation, DIA brought together international law enforcement agencies including the FBI, the Australian Federal Police, the Royal Canadian Mounted Police, the National Crime Agency in the UK, Europol and INTERPOL, as well as NZ Police and New Zealand Customs Service to establish a co-ordinated approach to identifying and investigating individuals tied to these accounts.

What followed was hundreds of investigations, commenced across the world.

From February 2020 onwards DIA and NZ Police, along with intelligence assistance from New Zealand Customs Service, undertook warrants and prosecutions into the New Zealand based offenders.

To date 125 New Zealand based accounts have been identified as part of the investigation. Due to the number of user accounts identified and the extreme egregious nature of the child sexual abuse material involved, this is the most significant joint child sexual exploitation operation conducted within New Zealand.

Tim Houston, Manager Digital Child Exploitation Team, and lead for Operation H highlighted how this operation and the prosecutions that will follow represent a major success in international efforts to undermine and disestablish the environments and networks that seek to exploit children.

"I commend the ongoing support of our law enforcement partners domestically and across the world for their dedication

and hard-work. This operation will have an impact on the global networks that deal in the most horrific and damaging material, and we are extraordinarily proud of the effect it will have on children's lives around the world."

He also noted the real-world consequences of this sort of offending.

"Many people who view material of this kind will go on to physically offend against children, it is imperative that we are able to bring them to justice before they are able to do more damage. This is not a victimless crime, every time this material is viewed, that child is revictimized."

Houston went on to highlight the importance of collaboration in an operation like this.

"This is one of the largest investigations of online child sexual abuse conducted in the Department's history. I applaud the great work of our partner agencies in NZ Police and New Zealand Customs Service for their continued support. This is yet another excellent example of cross agency collaboration in Aotearoa. I cannot express the importance that the joint agency cooperation had on an operation of this scale."

As part of this operation the Digital Child Exploitation Team seized and examined hundreds of thousands of child abuse material files. The child sexual abuse material at the core of this investigation is some of the most egregious investigators have been exposed to. Many of the children featured in the images and videos were just infants who were exposed to obvious and intentional pain and suffering.

The two-year long operation has also produced the following results:

- 46 New Zealand based individuals arrested
- 836 cases investigated internationally
- 146 children safeguarded internationally

This Operation serves as a warning to other offenders preying on children online and distributing child exploitation material, that this will not be tolerated in New Zealand. DIA, NZ Police and New Zealand Customs Service will continue to prosecute to the fullest extent of the law and individuals who create, view and distribute this type of material will be found and held to account for their offending.

If you are concerned that something you have seen may be objectionable or want to report a crime, you can report it to the Digital Child Exploitation team at DIA.

If you are the victim of a child abuse or sexual abuse crime call Safe to Talk: 0800 044 334 Text 4334

Or access the Child Abuse: Directory for information and support

If you are concerned about a child or young person who could be a victim of abuse call Police on 105 or provide information to Police via Crimestoppers on 0800 555 111. You can also contact Oranga Tamariki on 0508 FAMILY (0508

326 459).

If you are concerned about your own activity online or someone else's sexual behaviour, you should contact organisations such as:

- Safe Network: 09 377 9898
- WellStop: 04 566 4745
- STOP: 03 353 0257

Or local treatment providers, or specialist therapists.

The Department of Internal Affairs uses the term child sexual abuse imagery. The term child pornography downplays the harm of child sexual abuse.

ENDS

See all DIA websites See all DIA social media sites

---

www.govt.nz

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	Case No. 1:20-CR-143
v.	)	
	)	Honorable T.S. Ellis, III
ZACKARY ELLIS SANDERS,	)	
	)	Sentencing: April 1, 2022
Defendant.	)	
	)	

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION FOR NEW TRIAL AND TO RECONSIDER MOTIONS TO COMPEL AND SUPPRESS

The United States of America, by and through undersigned counsel, files this response in opposition to the defendant's motion for a new trial and to reconsider his repeated failed motions to compel and suppress. Dkt. No. 585. For the reasons below, the defendant's motion should be denied. Further, given the Court's familiarity with this case and the baselessness of the defendant's claims, a hearing on his motion would not aid the Court and is not necessary.

BACKGROUND

As explained in the search warrant affidavit, the investigation of the defendant began when the Federal Bureau of Investigation ("FBI") received a tip from a foreign law enforcement agency ("FLA") that his Internet Protocol ("IP") address was used on May 23, 2019 to access "child sexual abuse and exploitation material" on a hidden service on The Onion Router network ("Tor," also known as the "dark web") dedicated to depictions of violent child sexual abuse ("Target Website"). Dkt. No 252-1 ("Affidavit") at ¶ 23. The FLA advised that it obtained this information through its own lawful, independent investigation without interfering with any computer in the United States. *Id.* at ¶ 25. And as explained in another section of the Affidavit, the server containing the Target Website was seized by a foreign law enforcement agency in June 2019, after the defendant's IP

address was used to access child sexual abuse material on the site. *Id.* at ¶ 15. The agency that seized the server is not the FLA described in paragraphs 22 through 26 of the Affidavit that conducted the investigation that led to the information in the tip.

The defendant was later charged in a twelve-count indictment with production, receipt, and possession of child pornography. Dkt. No. 29. He proceeded to trial, and, on October 27, 2021, a jury found him guilty of all counts. Dkt. No. 541. On November 4, 2021, he moved to continue the deadline for filing post-trial motions to January 9, 2022. Dkt. No. 543. The Court extended the deadline to December 27, 2021, but he did not file any timely briefing. Dkt. No. 544. On January 20, 2022, another attorney joined the defense, bringing the number of attorneys who have appeared on behalf of the defendant in this case to nine. Dkt. No. 566. That same day, the defendant's newest attorney filed a motion to continue the sentencing, citing the need to have the defendant evaluated by multiple doctors. Dkt. No. 569. The Court initially denied the motion, Dkt. No.572, but later postponed the sentencing from March 4, 2022, to April 1, 2022, Dkt. No. 581.

On March 3, 2022, a different defense attorney sent undersigned counsel a transcript from a September 17, 2021 hearing on a motion to compel (Dkt. No. 586-1, "*Kiejzo* transcript,") and a complaint affidavit filed on January 28, 2020 (Dkt. No. 586-5), and asked if it is "accurate that the information underlying the tip was from an unnamed FLA," and if there is any exculpatory evidence regarding the defendant's activity on the Target Website. *See* Dkt. No. 586-8. Undersigned counsel responded that his claim about an unnamed foreign agency was inaccurate, and that law enforcement could not further investigate the defendant's activity on the Target Website because he did not provide his username. *Id.* Ignoring this response, defense counsel insisted that the country that seized the server—not the FLA—conducted the investigation that uncovered the information in the FLA's tip based on the *Kiejzo* transcript. *Id.* Undersigned counsel

reiterated that the tip came from the known FLA and the information in the tip came from that FLA's independent, lawful investigation. *Id.* Undersigned counsel also advised that the defense's claim to the contrary was based on the defense's unsupported claim in *Kiejzo* that conflates the seizure of a server with how the FLA obtained the information in the tip in that case.[1] *Id.*

On March 14, 2022, the defendant filed the instant motion requesting that the Court order a new trial under Federal Rule of Criminal Procedure 33 ("Rule 33") and reconsider its rulings on approximately 28 pre-trial motions and filings. *See* Dkt. No. 586 at 1 n.1. Attached to his motion are hundreds of pages of exhibits, which he submits in an attempt to supplement his prior failed claims for an appeal. Dkt. No. 586 at 1, Dkt. Nos. 586-1 to 586-45. The Court ordered the government to respond on or before March 18, 2022. Dkt. No. 587.

ARGUMENT

Prior to trial, the defendant filed dozens of motions and "supplements" raising a litany of claims, many of which were untimely and all of which were denied. His latest motion—totaling over 700 pages in briefing and exhibits but providing no substantive evidence that was not available prior to the trial—is no different. Indeed, he filed it around 77 days after the already-extended motions deadline and less than three weeks after he obtained a continuance of the sentencing on other grounds, and it should therefore be denied as untimely. Dkt. Nos. 544 & 582.

Moreover, his latest motion appears to be the result of his collaboration with defendants in other cases, as he is now advancing the failed argument of another defendant alongside untimely

[1] In the *Kiejzo* transcript, the court criticized the defendant's argument as speculative and denied the defense motion to compel in an order that was made public on October 12, 2021. Dkt. No. 586-1; *see also* Ex. 1 (*United States v. Kiejzo*, Criminal No. 20-40036, Order, Dkt. No. 106-1 (D. Mass. Oct. 4, 2021). Based on the order, it appears that the defendant in that case asked whether the country that seized a server containing two websites was the same FLA that provided the tip in his case, and the government advised that it was not. Nowhere does the government state that the country that seized the server also de-anonymized the defendant's IP address and told the FLA.

arguments this Court has already rejected. And while his wide-ranging claims are untethered from any unifying argument or principle, his motion at base challenges whether the Affidavit established probable cause to search his home and not any issues from the trial. In particular, it relates to two paragraphs in the Affidavit stating that the FLA provided a tip that the user of his IP address accessed "child sexual abuse and exploitation material" on the Target Website, that the FLA has a history of providing reliable information, and that the FLA advised that it obtained this information through its own independent, lawful investigation without interfering with any computer in the United States. All this information is documented in the tip, which has been extensively litigated. Nothing in his latest motion supports his "conspiratorial" theories that the tip is false or misleading, that the FBI knows or believes the tip is false or misleading, or that the United States is withholding exculpatory material related to the tip or the Affidavit. Dkt. No. 369 at 6. His claims are instead based on "a stack of hypotheticals" that he is insisting the government must disprove even though he knows that the same or similar theories have been rejected by this Court and other courts. *See, e.g.*, *United States v. Bateman*, Criminal Action No. 1:20-cr-10012-IT, 2021 WL 3055014, at *3 (D. Mass. July 20, 2021). Accordingly, his motion should be denied.

I. The Defendant's Motion for a New Trial is Not Based on New Evidence Discovered through the Exercise of Due Diligence and is Untimely

As an initial matter, despite framing his motion as based on newly discovered evidence pursuant to Rule 33(b)(1), the defendant's request for a new trial relies on information that was available to him prior to trial and his motion should be denied as untimely. Pursuant to Rule 33(a), the Court may "vacate any judgment and grant a new trial if the interest of justice so requires." The Fourth Circuit has instructed that "[a] trial court should exercise its discretion to award a new trial sparingly," and "a jury verdict is not to be overturned except in the rare circumstance when the evidence weighs heavily against it." *United States v. Williams*, 783 F. App'x 269, 274 (4th Cir.

2019) (internal citation omitted)). When a defendant seeks a new trial based on allegedly new evidence, he bears a heavy burden. To obtain a new trial in those circumstances, the defendant "must satisfy a five-part test by showing that (1) the evidence is newly discovered; (2) the defendant exercised due diligence; (3) the newly discovered evidence is not merely cumulative or impeaching; (4) the evidence is material; and (5) the evidence would probably result in acquittal at a new trial." *United States v. Moore*, 709 F.3d 287, 292 (4th Cir. 2013) (citing *United States v. Chavis*, 880 F.2d 788, 793 (4th Cir. 1989)). "And, in the absence of a *Brady* violation, 'a new trial should be granted only when the evidence weighs heavily against the verdict.'" *United States v. Lobo-Lopez*, No. 1:08-cr-194-TSE, 2010 WL 11691673, at *1 (E.D. Va. May 25, 2010) (quoting *United States v. Arrington*, 757 F.2d 1484, 1486 (4th Cir. 1985)).

At the defendant's request, the Court set the deadline to file Rule 33 motions as December 27, 2021. Dkt. No. 544. He filed the instant motion on March 14, 2022, referencing "newly discovered materials" with no other explanation as to why he failed to comply with that deadline. Dkt. 586 at 2. But "[n]ewly discovered evidence means evidence discovered since the trial," *Moore*, 250 F.3d at 250, and the defendant's motion relies on materials from other matters that have been available since 2020 and 2021, if not earlier. And while he claims that the *Kiejzo* transcript in particular was not available until January 10, 2022, Dkt. 586 at 8 n.5, the court in *Kiejzo* denied the motion to compel from that hearing in an order that was made public on October 12, 2021, *see* Ex. 1, the defense in that case filed publicly available objections to that order that the defendant cites in his motion on October 18, 2021, Dkt. No. 856-2, and the defendant has been sharing information and affidavits from this case with the defense in that case since before the deadline to file post-trial motions here, Dkt. No. 586-6. Moreover, the *Kiejzo* transcript is not new evidence of anything. It certainly does not establish that an unknown country "deployed the

method that was used to obtain" the defendant's IP address, as he now claims. Dkt. No. 486 at 3. The government advised the defendant of this weeks ago, but he nevertheless filed the instant motion well after the deadline for post-trial motions. *Id.* at 10-11.

The only information referenced in the defendant's motion that appears to at least partially post-date the trial comes from assorted press releases, none of which have any clear bearing on the reliability of the FLA's tip or the accuracy of the Affidavit. Dkt. 856 at 25-27. It is unclear if these releases even refer to a related matter, as he acknowledges. *Id.* at 25 (guessing that investigation "appears" to relate to the FLA's investigation). The defendant made a similar argument about the government's alleged involvement with the FLA's investigation based on his parsing of other random press releases before, and the Court rejected the claim as "unsupported speculation." Dkt. No. 236 at 5-6. In sum, the "newly discovered evidence" the defendant relies on in his motion for a new trial is not newly discovered or even evidence relevant to this case at all. At a minimum, the same information was or could have been uncovered prior to the trial and certainly prior to the Court's deadline to file post-trial motions, and his motion should be denied.

II. The Defendant's Motion for a New Trial Fails Satisfy the Other *Chavis* Factors

Even if the Court determines that the defendant's motion for a new trial is timely and based on new evidence discovered through the exercise of due diligence, he still fails to satisfy the other *Chavis* factors required to warrant a new trial. His motion is simply an extension of his oft-used discovery tactic, in which he hypothesizes ways that the FLA's tip and the Affidavit might be false, repeats those suspicions as facts based on a patchwork of documents that do not actually support his far-reaching theories, and then faults the government for not proving these theories for him while discarding as "not accurate" any information contradicting them. Dkt. No. 586 at 10. Because his speculative claims do not change the fact that the Affidavit accurately conveyed the

FLA's tip and established probable cause to search his home, this allegedly new evidence in his motion is cumulative, immaterial to any relevant issue, and unlikely to result in an acquittal.[2] Accordingly, his motion for a new trial should be denied.

The defendant first claims that a transcript from one case and a plea agreement from another prove that an unknown country de-anonymized his IP address and gave it to the known FLA, which "merely provid[ed] that information second-hand" to the FBI with no independent investigation, contrary to the FLA's tip. Dkt. No. 586 at 2-3, 7-10. The government struggles to understand this claim because, put simply, there is no good-faith reading of the documents that supports it, let alone proves it. With respect to the *Kiejzo* transcript, the defendant simply parrots the defense's speculative claim from that hearing, which that court rejected. *Supra* p.3 n.1. Further, the cherry-picked, generic sentence from the plea agreement—"Law enforcement infiltrated this dark web website and determined that the defendant had utilized the website"—in no way proves that an unknown country obtained the information in the FLA's tip. *Id.* at 9-10. And even assuming these documents provide some support for his efforts to conflate the seizure of a server with the FLA's independent investigation and tip—which they do not—the defendant provides no support for the many other inferences required to make this claim material to a challenge to the Affidavit, including, at a minimum: that the seizing country's actions were unlawful and violated his rights; that the FLA that provided the tip knew this and misrepresented the origin of the tip; and that the FBI also knew this and was working with one or more foreign agencies to conceal this. The only

[2] In fact, because the defendant's motion is directed exclusively at so-called "newly discovered evidence" allegedly affecting the reliability of the FLA's tip and the validity of the Affidavit—and not any evidence that could have been presented at trial—his motion for a new trial necessarily fails to identify material that would likely have resulted in an acquittal and should be denied on this basis alone (in addition to relying on material that is neither "newly discovered" nor relevant to either the existence of probable cause in the Affidavit or the government's discovery obligations). *See Moore*, 709 F.3d at 292.

"evidence" for these claims beyond the defendant's baseless assertions are the equally baseless assertions made by another defendant. *See also Bateman*, 2021 WL 3055014, at *3-4 ("All of Bateman's requests are based entirely on speculation that the evidence may show wrongdoing by foreign and domestic law enforcement.").

The government corrected the defendant's misunderstanding prior to the filing of this motion, confirming that the statements in the Affidavit about his IP address came from the same reliable FLA that has been the subject of his prior motions and that this FLA advised that it collected this data through an independent and lawful investigation. Dkt. No. 586-8. The defendant ignored the government and filed the instant motion, alleging in conclusory fashion that the government's communication was "not accurate."[3] Dkt. No. 586 at 10. But despite his claim to the contrary, the defendant has not identified anything beyond his own speculation—and now the speculation of another defendant—to prove the inaccuracy of the sworn Affidavit and show that "the tip no longer has any indicia of reliability." *Id.* at 10-11. The defendant's allegedly new evidence is therefore cumulative of his many speculative pre-trail motions, immaterial, and unlikely to produce an acquittal, and his motion for a new trial should be denied.

The defendant next claims that he is entitled to a new trial because he believes the government has exculpatory evidence regarding his activity on the Target Website. Dkt. No. 586 at 15-16. His claim is based on an out-of-district complaint filed in January 2020, which describes what appear to be archived postings on a Tor site obtained after a defendant provided, among other information that may not be disclosed in the complaint, his username and password to the site. *See*

[3] The defendant's total disregard of the government's effort to correct his false understanding of the Affidavit underscores the frivolousness of his repeated accusations that the government "fail[ed] to correct" other false impressions he held. Dkt. No. 586 at 10-11. Even assuming that the government bears the responsibility to correct every false belief to which the defendant unjustifiably clings, his motion itself makes clear the fruitlessness of any such effort.

Dkt. 586-5 at ¶ 13. As the government also explained to the defense, law enforcement cannot further investigate his activity on the Target Website because he did not provide his username on the site, though he admitted to downloading child sexual abuse material from sites like the Target Website. If the defendant wishes to provide his true username and password—which he is unlikely to do now—the government can further investigate his criminal activity. More to the point, whether the defendant engaged in additional activity on the Target Website is immaterial because the Affidavit as written establishes probable cause.[4] *See* Dkt. No. 113. Accordingly, to the extent the information in this two-year-old complaint is new, it is cumulative, immaterial to the narrow probable-cause dispute raised in the defendant's motion, and unlikely to result in an acquittal. The defendant's motion for a new trial on this ground should therefore be denied as well.

The defendant's remaining grounds for a new trial are either recycled versions of his failed arguments or new arguments that he failed to timely raise. In either instance, they are frivolous. He claims, for example, that affidavits in support of search warrants from other cases prove that the Affidavit here lacked probable cause. Dkt. No. 586 at 12-14. That is, of course, incorrect. Information in affidavits not before the magistrate judge are immaterial to a court's probable cause determination. *See United States v. Montieth*, 662 F.3d 660, 664 (4th Cir. 2011) ("The magistrate's probable cause determination is a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him there is a fair probability that contraband or evidence of a crime will be found in a particular place." (internal alterations removed)); *id.*

[4] The defendant also relies on the complaint to make wide-ranging and unsupported claims about the FBI's purported ability to de-anonymize users and further investigate activity on the Target Website. Dkt. No. 586 at 7, 15-16. The limited information in the complaint does not support the defendant's conclusory assertions. Moreover, as explained above, whether the defendant engaged in additional activity on the Target Website is irrelevant because the information already included in the Affidavit—including the reliable FLA's tip—is sufficient to establish probable cause.

(limiting review of magistrate judge's determination to whether there was a "substantial basis for determining the existence of probable cause"). He also argues that these other affidavits, some of which were prepared by Homeland Security Investigations, prove the FBI did not think the Affidavit here established probable cause. Dkt. No. 586 at 12. The defendant's suggestion that a handful of warrants from other cases are somehow representative of the FBI's views on the Affidavit in this case is absurd. It is also belied by the record, which reflects that both Magistrate Judge John F. Anderson and this Court agreed that the warrant established probable cause.

He also claims that the affidavits and heavily redacted reports from other investigations confirm that the government has been investigating the Target Website for years, that a Network Investigative Technique ("NIT") must have been used to identify his IP address, and that the FBI was engaged in a joint investigation with whoever used a NIT and hid this information. Dkt. No. 586 at 17-22. The defendant has long known, however, that law enforcement in the United States was also investigating the Target Website, that law enforcement received other tips, and that a Tor user's IP address can be de-anonymized without a NIT. *See, e.g.*, Dkt. No. 350 at 3 n.2; Dkt. No. 101 at 23. Additional confirmation that the government is investigating others based on similar tips is simply cumulative of evidence he already has and immaterial to the probable-cause issue in his motion. Nor does the fact that the government gleaned information about individuals who accessed child sexual abuse material on a Tor hidden service in a prior investigation that involved a NIT confirm the defendant's ongoing suspicion that a NIT was used here. *Id.* at 21-22. Similarly, the fact that the Affidavit included information about registered users of the Tor site from this prior investigation does not magically render the Affidavit's accurate description of the FLA's tip misleading. *Id.* at 23-24. These arguments are non sequiturs. Moreover, they are variations of

arguments he already raised, and he is not entitled to litigate the validity of the Affidavit again with no new evidence by repackaging his theories in a motion for a new trial.

Finally, the defendant asserts that various press releases prove the FBI was "working hand in hand" with other countries to bolster his claim that the FBI was engaged in a joint venture and was therefore a "party to an imagined Fourth Amendment violation alluded to in defendant's previous motions to suppress." Dkt. No. 236 at 6. The Court has twice rejected this claim as speculative and untimely, *see id.* & Dkt. No. 501 at 3, and nothing in the defendant's latest motion changes this. In fact, he admits that he does not know if the documents he found online even relate to the FLA's tip and is relying on perceived similarities in names to support his theory. Dkt. No. 586 at 25. He cannot point to a single press release establishing that the FBI knows or should know information undermining the FLA's tip or that the FBI had any involvement with any of these investigations beyond receiving the tip. The defendant's argument is more of the same rank, untimely speculation that this Court previously denied, and the defendant's motion for a new trial on this ground should be denied, too.[5]

[5] As he has done throughout this case, the defendant filed a last-minute "supplemental" brief in support of his exceedingly untimely joint-venture claim and attached what he asserts are a foreign report and transcript to prove it. Dkt. No. 591. The supplement is, put bluntly, conspiratorial gibberish. He has provided no additional information as to what these documents are, who edited and provided them, or why they appear to have been photographed on a towel, but even assuming they are what he says they are, they do not prove his "supplemental" theory that the FBI engaged in a joint venture to operate the Target Website for years, all while repeatedly deploying NITs that captured his IP address. *Id.* at 3. As best the government can tell, an individual who was prosecuted in another country years ago for his proven involvement with different sites once made a reference to the Target Website to law enforcement. Dkt. No. 591-2 at 2. Neither document appears to make any other mention of the Target Website, nor any mention at all of the FBI, the concept of a NIT, or any investigative activity taken after 2017. To be sure, law enforcement agencies around the world are working—sometimes together, sometimes alone, and often at the same time—to take down websites that traffic in the kind of violent child sexual abuse material that the defendant enjoys. How he concluded that his supplemental brief proves the existence of a joint venture here, however, is a mystery, and his motion should be denied.

III. The Defendant's Motion to Reconsider his Repeated Failed Motions to Compel and Suppress is Untimely and Should Also be Denied

The defendant also asks the Court to reconsider (for at least the fifth time, based on a review of the docket) its rulings on his pre-trial motions to compel and suppress. The Court has made clear that "a motion for reconsideration can be successful in only three situations: (1) to accommodate and intervening change in controlling law; (2) to account for new evidence; or (3) to correct a clear error of law or prevent manifest injustice." Dkt. No. 501 at 2 (citing *Zinkland v. Brown*, 478 F.3d 634, 637 (4th Cir. 2007)). The defendant appears to be relying on the new-evidence prong to support his latest motion. But for the reasons above, the evidence he relies on is not new and was known or should have been known to him through the exercise of reasonable diligence prior to the trial. *Supra* pp. 5-7. Accordingly, his motion for reconsideration should be denied. *See* Dkt. No. 107 (explaining that a motion to reconsider must be based on evidence unavailable at trial); *see also United States v. Dickerson*, 971 F. Supp. 1023, 1024 (E.D. Va. 1997) ("In order to support a motion for reconsideration, the movant is obliged to show not only that ... evidence was newly discovered or unknown to it until after the hearing, but also that it could not with reasonable diligence have discovered or produced such evidence at the hearing.").

To the extent the evidence is new, the defendant is asking this Court to "rethink what the Court ha[s] already thought through—rightly or wrongly." *Dickerson*, 971 F. Supp. at 1024 (internal quotation marks omitted). As described above, the Court has repeatedly rejected the claims in his motion, including that: the FBI knew that a NIT was used; the FBI was engaged in a joint venture; the government misled the defendant and the Court about the scope of the investigation; and the Affidavit's description of the FLA's tip is misleading. *See, e.g.*, Dkt. Nos. 73, 107, 113, 236, 442, 501. Repurposing these arguments under the guise of "newly discovered" information that in reality is cumulative of the same failed claims he has repeatedly advanced does

not require a different outcome, nor does it "resolve[ ] the serious issues of timeliness that have plagued all of defendant's motions[.]" Dkt. No. 501 at 3.

Finally, even if the Court reaches the merits of the defendant's motion, he has failed to show that he is entitled to additional discovery or that the Affidavit was invalid. Instead, as he has done before, he has invented ways in which the FLA's tip might be unreliable or there might be exculpatory evidence and insisted that the government provide the evidence to support those very claims. But the defendant's "repeated incantation that the government misrepresented the FLA's tip does not make it so," Dkt. No. 73 at 10-11. His reliance on the *Kiejzo* transcript is more of the same. The *Kiejzo* transcript does not prove that an unknown country "deployed a technique that identified [the defendant's] IP address" and the FBI knew this. Dkt. No. 586 at 28. Rather, it captures the uninformed speculation of a defendant who, like the defendant here, is grasping at straws to undermine what the FLA's tip plainly states. Omitted entirely from his motion is the order from the court that heard this argument, which describes the claim now advanced by the defendant as "speculation" and supported only by the "bald assertion of a possibility." Ex. 1 at 6-7. The defendant cannot launder what he knows to be baseless, failed arguments from another defendant through a motion for reconsideration, and his motion should be denied.

The government has complied with its discovery obligations. That the government did not catch and correct the defendant's unsupported and irrelevant inference about the seizure of the Target Website's server in a few of his many filings does not prove that "there is a significant amount of withheld discovery material." Dkt. No. 586 at 28. Indeed, the instant motion is so rife with inaccuracies, distortions, and baseless inferences that the government would be hard-pressed to address them all in a single filing. Nor should the government have to. The burden is on the defendant here, and he cannot satisfy that burden by repeatedly seeking to delay the resolution of

this case and then inundating the Court with speculative claims that ignore the evidence before him. While this is not the first time he has exploited the litigation process in this way, the frivolousness of the instant motion is particularly clear given that he was informed that his arguments were premised on a misapprehension of the facts. *See also* Dkt. No. 369 (denying motion to compel the production of material he had already been told does not exist). Because the defendant has only offered non-conclusory allegations to support the many logical leaps required to show the materiality of his claims, his motion should be denied.

CONCLUSION

The government respectfully requests that the Court deny the defendant's motion for a new trial and to reconsider his failed motions to compel and motions to suppress. Dkt. No. 585.

Respectfully submitted,

Jessica D. Aber
United States Attorney

By: /s/

William G. Clayman
Special Assistant United States Attorney (LT)
Jay V. Prabhu
Seth M. Schlessinger
Assistant United States Attorneys
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700

CERTIFICATE OF SERVICE

I hereby certify that on March 18, 2022, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of that electronic filling (NEF) to counsel of record.

By: /s/

William G. Clayman
Special Assistant United States Attorney (LT)
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
Email: william.g.clayman@usdoj.gov

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	Criminal No. 20-40036-TSH
VINCENT KIEJZO,	)	
	)	
	)	
Defendant	)	
	)	
	)	

ORDER ON MOTION FOR DISCOVERY

October 4, 2021

Hennessy, M.J.

Defendant is charged by indictment with one count of Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). He has moved to compel discovery which the parties briefed and argued at an in-person hearing. For the reasons that follow, the motion is denied.

I. Factual and Procedural Background

On September 8, 2020, DHS special agent Caitlin Moynihan applied for a warrant for Defendant's residence. [Dkt. No. 2-3]. Her supporting affidavit alleged probable cause to believe that a computer in Defendant's home accessed two child pornography websites, Website 2 and Website 3, operating on the TOR network. [Dkt. No. 80-6, ¶ 5]. Among other averments, Moynihan presented information about the content of Websites 2 and 3, including detailed descriptions of images of child pornography found there, topics available to users, and user posts. [Id. ¶¶ 15–29]. Moynihan averred that the TOR network, on which these websites operated, is designed to anonymize the IP addresses which access TOR network websites by routing internet

communications through a path of random IP addresses before reaching a destination computer, as well as the IP addresses hosting services on the TOR network that users may access. [Id., ¶¶ 7–8, 14]. Moynihan noted that hidden service websites on the TOR network are not indexed or easily identified by search engines, such as Google, and generally a user would need to take deliberate steps to access Website 2 or Website 3, including knowing and inputting the 16 or 56-character web address for either. [Id. ¶ 35]. Thus, while the TOR network does not guarantee anonymity for a user accessing its hidden services, the routing of communications through a path of IP addresses makes traditional identification techniques largely ineffective. [Id. ¶¶ 7, 11]. Given the anonymity the TOR network creates, and that TOR hidden service websites are accessible to users anywhere in the world, it is common for law enforcement agencies from investigating countries to share information relevant to an offender or a site in other countries. [Id. ¶ 35].

According to Moynihan, in June 2019 a foreign law enforcement agency ("FLA") seized the computer server(s) located outside the U.S. which hosted Website 2 and Website 3. [Id. ¶¶ 15, 23]. In August 2019, an FLA "known to U.S. law enforcement and with a history of providing reliable, accurate information" notified U.S. law enforcement that it had determined that IP address 96.230.213.63 (the "96 IP address") had accessed Website 2 on May 12, 2019 at a certain time, and Website 3 on the same date about 16 minutes thereafter. [Id. ¶¶ 31–32].[1] Moynihan averred the notifying FLA was "a national law enforcement agency of a country with an established rule of law;" that the FLA and U.S. law enforcement had a long history of criminal information-sharing; that the notifying "FLA advised U.S. law enforcement that it had obtained [the IP] information through independent investigation that was lawfully authorized in the FLA's country pursuant to

[1] The Government disclosed in discovery that the notifying FLA, the [redacted], was not the seizing FLA. [Dkt. No. 80, p. 1 n.1].

its national laws;" that in doing so the "FLA had not interfered with, accessed, searched, or seized any data from any computer in the [U.S.] in order to obtain the IP address information;" and that U.S. law enforcement "did not participate in the investigative work through which the FLA identified the IP address." [Id. ¶ 33]. Moynihan recounted that prior tips associated with TOR network child exploitation websites from the notifying FLA led to the identification and arrest of a U.S.-based producer of child pornography and hands-on offender, and rescue of child victims of this offender; the seizure of evidence of child pornography trafficking and possession; and corroboration for information independently developed of child pornography trafficking and possession. [Id. ¶ 34].

On March 20, 2020, agents issued an administrative subpoena to Verizon Fios for customer information for the user of the 96 IP address on the date and times provided in the tip. [Id. ¶ 39]. Verizon reported the 96 IP address belonged to Defendant's residence. [Id.]. Agents executed the warrant on September 9, 2020. [Dkt. No. 2-3, ¶ 5]. In Defendant's bedroom, agents located a thumb drive which contained 6,000 video files, including files depicting minors engaged in sexually explicit conduct, and a document with four links to the TOR network. [Id. ¶¶ 9–10]. Defendant was present, waived his Miranda rights, and when informed of what agents had located admitted possessing child pornography on the thumb drive and accessing the TOR network. [Id. ¶¶ 12–13].

Following indictment and the Government's discovery production, Defendant requested additional discovery, some of which the Government provided. As noted, during discovery, the Government advised Defendant that the FLA which seized the servers hosting Websites 2 and 3 was not the notifying FLA [redacted] [Dkt. No. 80, p. 1 n.1]. Defendant then moved to compel discovery and for an in-person hearing on the motion. Defendant alleged that the discovery he

sought to compel was required under Fed. R. Crim. P. 16, Local Rules 116.1 and 116.2, Brady v. Maryland, 373 U.S. 83 (1963), the Fifth Amendment, and Defendant's ability to prosecute a hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1978). [Dkt. No. 80].

II. Legal Standard

Rule 16 of the Federal Rules of Criminal Procedure directs the government, upon a defendant's request, to allow a defendant to inspect and copy any item in the government's possession, custody, or control that is either (i) material to preparing the defense; (ii) an item the government intends to use in its case-in-chief at trial; or (iii) was obtained from or belongs to the defendant. See Fed. R. Crim. P. 16(a)(1)(E). As to the first category, a defendant, as the moving party, bears the burden of showing materiality. United States v. Goris, 876 F.3d 40, 44 (1st Cir. 2017). "A showing of materiality requires 'some indication' that the pretrial disclosure of the information sought 'would have enabled the defendant significantly to alter the quantum of proof in his favor.'" Id. (quoting United States v. Ross, 511 F.2d 757, 763 (5th Cir. 1975)). A significant alteration may occur in myriad ways, including "uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." Id. (quoting United States v. Lloyd, 992 F.2d 348, 351 (D.C. Cir. 1993)). However, a showing that what is sought bears some abstract relationship to the issues in the case is not enough. Id.

Local Rule 116.1 does not add much for purposes of this motion; it requires the government to produce all information to which a defendant is entitled under Rule 16. See Local Rule 116.1(c)(1)(A). In relevant part, Local Rule 116.2 implements Brady v. Maryland, 373 U.S. 83 (1963) and its progeny, and defines exculpatory evidence to include information which tends to cast doubt on: a defendant's guilt or any essential element of a charged offense; the admissibility of evidence that the government may offer in its case-in-chief; the credibility or accuracy of

evidence the government may offer in its case-in-chief; or information that tends to diminish a defendant's culpability. See Local Rule 116.2(a).

Finally, Defendant claims the discovery is needed for him to prosecute a Franks hearing. In Franks v. Delaware, the Court said:

> There is, of course, a presumption of validity with respect to the affidavit supporting the search warrant. To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. . . . The deliberate falsity or reckless disregard whose impeachment is permitted today is only that of the affiant, not of any nongovernmental informant.

438 U.S. at 171. Entitlement to discovery to mount a Franks challenge requires the same substantial preliminary showing. See United States v. Long, 774 F.3d 653, 661–62 (10th Cir. 2014) (disclosure of informant not required where defendant's allegations consisted solely of speculation and failed to make the substantial preliminary showing required by Franks); United States v. Messalas, 17-cr-339 (RRM), 2020 WL 1666162, at *11 (E.D.N.Y. Apr. 4, 2020) ("Messalas cannot seek discovery to support his Franks challenge without first making the preliminary showing required to grant a Franks hearing"); United States v. Harding, 273 F. Supp. 2d 411, 430 (S.D.N.Y. 2003) (where defendant failed to make the substantial preliminary showing for a Franks hearing, he is not entitled to "wide-ranging discovery to canvass for evidence to support his motion to suppress."); cf. United States v. Koschtschuk, 09-cr-0096(S)(M), 2011 WL 1549464, at *1–2 (W.D.N.Y. Apr. 22, 2011) (explaining that if a defendant makes the threshold showing in support of a Franks hearing, discovery may be allowed).[2]

[2] Defendant fails to develop the claim that the Fifth Amendment requires disclosure. The claim is therefore waived. See United States v. Zanino, 895 F.2d 1, 17 (1st Cir. 1990) (issues averted to in a perfunctory manner, unaccompanied by some effort at developed argument, are deemed waived).

III. Analysis

With this law in mind, Defendant moves for the following discovery:

> *#3-4: The identity of the FLA that seized the computer server hosting Websites 2 and 3 in June 2019, as referenced in ¶¶ 15-16 of the Affidavit.*
>
> *#8: Any record of the investigative technique(s) utilized by the FLA with respects to the "notification(s)" described in ¶¶ 31-33 of the affidavit.*

[Dkt. No. 80, pp. 17, 20]. The Government has declined to disclose this information. I find that Defendant has failed to show the relevance or materiality of the requested discovery. As an initial matter, Defendant can prosecute a motion to suppress without this discovery. Indeed, review of the sufficiency of the probable cause is limited to the four corners of the affidavit. Aguilar v. Texas, 378 U.S. 108, 109 n.1 (1964), abrogated on other grounds by Illinois v. Gates, 462 U.S. 213 (1983). The seizing FLA is not identified in Moynihan's affidavit; hence, its identity is not relevant to resolution of a motion to suppress.

Defendant nevertheless relies on two exceptions to the purely domestic scope of the exclusionary rule to compel production. "Ordinarily, the Fourth Amendment's exclusionary rule does not apply to foreign searches and seizures, for 'the actions of an American court are unlikely to influence the conduct of foreign police.'" United States v. Valdivia, 680 F.3d 33, 51 (1st Cir. 2012) (quoting United States v. Hensel, 699 F.2d 18, 25 (1st Cir. 1983)). "There are, however, two well-established exceptions to this rule: (1) where the conduct of foreign police shocks the judicial conscience, or (2) where American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." Id. (quoting United States v. Mitro, 880 F.2d 1480, 1482 (1st Cir. 1989)). Defendant has failed to proffer any persuasive showing that the first exception applies. Rather, his argument appears to be that if the seizing FLA were identified, the seizing FLA's investigation might be identified, and it may be determined from review of the

investigation that the seizing FLA engaged in conduct which might shock the judicial conscience. This argument is, as it sounds, speculation and in the absence of an offer of proof that the seizure involved conduct that would shock a judicial conscience, fails to meet Defendant's burden.

In suggesting that the 96 IP address information was the product of a joint venture, Defendant assembles information which reflects a history of cooperation and collaboration between U.S. and foreign country law enforcement agencies. [Dkt. No. 80, pp. 4–7]. Defendant also points to the reliance on MLATs between the U.S. and foreign countries to facilitate cooperation in criminal investigations, and notes that adoption of the [redacted] reflects Congress' endorsement of the MLAT between the U.S. and [redacted] to facilitate such cooperation. In the Court's view, a history of collaboration and treaties does not persuade the Court that a joint venture occurred here. Indeed, Moynihan expressly averred that the U.S. did not participate in the investigative work through which the FLA identified the IP address. [Dkt. No. 80-6, ¶ 33]. While Defendant correctly argues that this statement does not preclude the possibility that the U.S. participated in other phases of the investigation, at the same time Defendant offers nothing but this bald assertion of a possibility. Moreover, if U.S. agents had participated in, for instance, the seizure of the websites server(s), common sense suggests that a FLA tip would have been unnecessary to alert agents of the activities of the 96 IP address; rather, U.S. agents would have possessed such information. See Illinois v. Gates, 462 U.S. 213, 238 (1983) (affidavit should be read in a practical, common-sense manner). Lastly, it seems equally unlikely that U.S. agents directed an investigation into what IP addresses accessed the websites, since, as noted in the affidavit, the hidden service websites on the TOR network are accessible globally and users may be located anywhere in the world, not necessarily or only in the U.S.

> ***#6-7:*** *The substance of the notification by the "FLA" to U.S. law enforcement regarding the identification of the IP address in this*

case, as referenced in ¶¶ 31-32 of the affidavit, including but not limited to:

a. the author of the "FLA" notification;
b. the identity of the "U.S. Law Enforcement" agency which received the notification and the recipient;
c. the complete content of the notification, including information on tactics and/or techniques utilized by the "FLA" to determine the identity of the IP address accessing the website;
d. any and all descriptions and/or identifications of Website 2 provided by the "FLA" in its tip to the U.S.;
e. the "further documentation" regarding Websites 2 and 3 provided by the FLA as referenced in ¶¶ 31-32 of the affidavit.

#9: *Any information, document, memorandum, and/or agreement addressing whether the FLA provided the information regarding the IP address in this case as part of a coordinated initiative or program with U.S. law enforcement.*

#16: *Any and all cover sheet(s), correspondence, and/or index list documenting the totality of "tip" and/or "notification" information provided by the FLA.*

[Dkt. No. 80, pp. 18, 20]. The Government produced photocopies of what the Court understands to be some of the communications from the notifying FLA that comprise the substance of the tip about the 96 IP address. These photocopies are heavily redacted, and Moynihan avers that the notifying FLA "provided further documentation naming [Website 2 and Website 3]" by their actual names and as having been accessed by the 96 IP address. [Dkt. No. 80-6, ¶¶ 31–32]. Defendant argues that complete copies of the documents comprising the tip should be produced, in part, to test the truthfulness of Moynihan's averments. [Dkt. No. 80, p. 13]. To support his preliminary discovery burden, Defendant takes issue with how the tip is described in the affidavit—the FLA "notified U.S. law enforcement" that the FLA had determined that at a certain time on a certain date the 96 IP address accessed Websites 2 and 3. Defendant infers that the tip was a single communication and, as such, would be in tension with the fact that there is no single piece of paper which links the 96 IP address to Websites 2 and 3. I disagree. Moynihan's averment summarizes the tip but does not detail how it was communicated. Further, Moynihan expressly averred that in seeking a search warrant, she did not include every fact known to her, but

only the facts she believed were necessary to establish probable cause. [Dkt. No. 80-6, p. 4]. For purposes of Franks discovery, I find that while the tip is drawn from several communications, read together these squarely identify Website 2 and Website 3 as hidden services on the TOR network which supported distribution of child pornography, and as having been accessed by the 96 IP address, and hence that Defendant fails to establish preliminarily a false or recklessly untrue averment. [Dkt. Nos. 80-7 to 80-9]. Defendant also points to a discrepancy between Moynihan's averment that the 96 IP address "accessed" the websites and the Government's statement in discovery that the 96 IP address "accessed or logged into" the websites to suggest a potential false or reckless statement. However, the Government readily conceded at oral argument that it spoke in error by including "logged into." In the Court's view, this argument makes too much of too little. As noted in the caselaw recited above, Defendant is not entitled to Franks discovery without making a substantial preliminary showing.

Defendant also argues that discovery is necessary to allow him to show that the investigation was a joint venture with U.S. law enforcement. [Dkt. No. 80, pp. 16, 19]. For the reasons stated above, I reject this argument.

Finally, I note that insofar as Defendant believes Moynihan's averments fail to link the 96 IP address to the websites, he can make such arguments in support of suppression.

> ***#10:*** *Complete copies of the "advisements" by the FLA to U.S. law enforcement regarding the "independent investigation" and "investigative work through which the FLA identified the IP address information" in this case, as referenced in ¶ 33 of the affidavit.*

[Dkt. No. 80, p. 21]. Having received photocopies of communications comprising the tip, Defendant trains this request on the seizing FLA and the possibility that the seizing FLA engaged in shocks-the-conscience misconduct. Because I find Defendant offers nothing but speculation to support this request, it is denied.

> ***#13:*** *The name of the "Operation," "Task Force," "Initiative," and/or organizing group assigned by the FLA to the investigation in this case, and the name of "Operation," "Task Force," "Initiative," and/or organizing group assigned by the FBI to the investigation in this case, if different.*
>
> ***#14:*** *The specific case FBI ID and/or serial number assigned to the Defendant's case.*

[Dkt. No. 80, pp. 21, 22]. Defendant offers myriad arguments to support production of this information. None of them is persuasive. He argues that the information is relevant to the nature and scope of the investigation and to showing whether there was a joint venture. For the reasons stated above, I find that Defendant has failed to submit a persuasive offer of proof that there was a joint venture here. I also reject the argument that names and numbers assigned to the case are material to defending this case.

Defendant also argues that the information is "necessary to determine whether there were any omissions and/or misstatements" in Moynihan's affidavit. [Dkt. No. 80, p. 21]. This argument ignores the settled law that Defendant must make a substantial preliminary showing for such discovery.

Lastly, Defendant makes the conclusory claim that information responsive to request 14 is Brady material. This claim is undeveloped and summarily rejected.

> ***#15:*** *Any record of action taken in response to the FLA notification by U.S. Law Enforcement agencies, including but not limited to copies of subpoenas and supporting materials (including spreadsheets, charts, lists, and/or other documents) sent to internet service providers, as referenced in ¶¶ 3 and 39 of the affidavit; and copies of returns to such subpoenas.*

[Dkt. No. 80, p. 23]. Insofar as Defendant argues that the Government should produce information regarding steps taken in other investigations in response to notifications from an FLA, such information is neither material nor relevant to Defendant's prosecution and is denied. Defendant further argues that there is a discrepancy between the action taken in this case between the subpoena to Verizon for information associated with the 96 IP address on the date and at the

times identified in the tip and Verizon's response which associates the 96 IP address with Defendant's residence not for only the date and times requested, but for the 10-month period in which the date and times occurred. This discrepancy is not significant. Accordingly, I deny the motion.

> ***#17:*** *With respect to the notification by the FLA to U.S. law enforcement:*
> *a. whether, and how, the FLA determined that the defendant's IP address accessed and/or visited a specific portion of Websites 2 and/or 3, and, if so, what specific portion of Websites 2 and/or 3 was accessed and/or visited;*
> *b. the number of tips provided by the FLA to U.S. law enforcement pursuant to its investigation under the United Kingdom's 2016 Investigatory Powers Act as referenced in its September 16, 2019 letter;*
> *c. the number of websites identified by the FLA to US. law enforcement pursuant to its investigation under the U.K.'s 2016 Investigatory Powers Act;*
> *d. the number of IP addresses identified by the FLA to U.S. law enforcement pursuant to its investigation under the U K. 's 2016 Investigatory Powers Act.*

[Dkt. No. 80, p. 24]. As to item (a), the Government reported that it is not in possession of information showing which portions of Websites 2 and 3 the 96 IP address accessed. Accordingly, the motion is denied as to item (a). As to items (b) through (d), Defendant argues that the responsive information is relevant to the scope of the investigation, and the method and reliability of the identification of the 96 IP address. In the Court's view, for purposes of this instant prosecution, the method and reliability of the identification of the 96 IP address depend on Moynihan's averments set forth in the four corners of her affidavit. Defendant has not made an offer of proof to warrant discovery to challenge in a Franks hearing the veracity of her averments. Defendant is of course free to argue that the averments fail to establish the reliability of the tipster, here the notifying FLA. Insofar as Defendant seeks items (b) through (d) to prove a joint venture, I find he has failed to make a showing to support the discovery requests.

IV. Conclusion

For the reasons stated above, Defendant's Motion to Compel Discovery [Dkt. No. 80] IS DENIED.

October 4, 2021

/s/ David H. Hennessy
David H. Hennessy
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant.	Case No. 1:20-cr-00143 Honorable T.S. Ellis, III Sentencing: April 1, 2022

NOTICE OF FILING OF SUPPLEMENTAL EXHIBITS

Zackary Ellis Sanders, by and through undersigned counsel, respectfully submits this notice of filing of supplemental exhibits to his Motion for New Trial and to Reconsider Motions to Compel and Motions to Suppress (ECF No. 585), which was filed on March 14, 2022. Since the defense filed its Reply (ECF No. 596) yesterday, it has learned of four additional cases that also arose from the same operation. These additional cases further corroborate Mr. Sanders's arguments in support of his Motions to Compel, Motions to Suppress, and Motion for a New Trial.

In *United States v. Holmstedt,* Case No. 2:21-CR-00004-JAG-RJK (E.D. Va., Dec. 8, 2020) (Affidavit in Support of Application for Issuance of a Criminal Complaint), attached as Ex. 1, the tip was provided by the foreign law enforcement agency (FLA) in August 2019; on September 11, 2019, an administrative subpoena was issued to Cox Communications; the FBI then sought a warrant for a pen register/trap and trace device, as opposed to a search warrant; and on June 23, 2020, a Magistrate Judge "authorized the installation and use of a pen register/trap and trace ('PRTT') device" for the Target IP address. *Id.* at ¶¶ 6-8. The PRTT device revealed

"evidence that a user of the internet [at the address] regularly accessed the Tor network, over a total of 200 times, beginning June 26, 2020, and continuing through August 21, 2020." *Id.* at ¶ 8. Only after the FBI corroborated the FLA's tip by confirming that the Internet user regularly connected to Tor did the FBI seek a search warrant for the residence. *Id.* at ¶ 9; *see also Holmstedt* Statement of Facts, attached as Ex. 2, at ¶ 1.

In *United States v. Edward Lewis*, Case No. 3:21-CR-00021-GEVT-EBA (C.D. Ky., Nov. 29, 2021) (Continuation Page/Supplementary Uniform Offense Report), attached as Ex. 3, the tip was provided in August 2019. *Id.* at 4. There, law enforcement had much more derogatory information regarding the suspect than it did here. The resident and owner of the suspect premises was a registered sex offender who had previously been convicted of four counts of Possession of Matter Portraying a Sexual Performance by a Minor. *Id.* at 9. Nonetheless, the FBI elected to conduct a knock and talk, as opposed to seeking a search warrant. During the agents' visit, Mr. Lewis admitted to going on Tor and agreed to a consensual search of his devices, during which the FBI uncovered child pornography. *Id.* at 9. Only then did the agents apply for a search warrant. *Id.* at 9-10; *see also Lewis* Search Warrant and Affidavit, attached as Ex. 4 (similar).

Lewis also reveals the following about the joint operation between U.S. law enforcement and FLAs:

> Homeland Security Investigations (HSI), working with foreign law enforcement and the Child Exploitation Operational Unit within the FBI, is investigating individuals accessing Dark Web sites/forums dedicated to the sexual abuse and exploitation of children. Through this investigation, law enforcement has identified hundreds of sexual abuse/child exploitation leads across the country. HSI Boston is working in conjunction with other HSI offices and jurisdictions to pursue warrants and prosecution of every target identified.

Ex. 2 (*Lewis* Report) at 1. This further corroborates that there are hundreds of searches that were conducted as a result of a single "investigation," in which U.S. law enforcement was working hand in hand with foreign law enforcement to take down the target website in this case and other websites on Tor. This shows there was full collaboration among HSI, the FBI, and FLAs, and that the government's narrow construction of the tip is an artificial, post-hoc one that is intended to mislead this Court and the defense about the nature of the operation that led to the identification and seizure of Mr. Sanders's IP address. The scale of this operation, including the hundreds of IP address leads that law enforcement pursued warrants and prosecutions for, further corroborates the defense's position that an NIT must have been used.

In *United States v. John Daniel Macintyre*, Case No. 1:21-CR-00121-JJM-LDA (D. RI., Mar. 17, 2021) (Criminal Complaint), attached as Ex. 5, the timeline of the tip and the FBI's initial investigation of the IP address followed the same timeline as this case, with the tip having been provided in August 2019 and a subpoena being issued to Cox Communications on November 22, 2019. *Id.* at ¶¶ 18, 26.

In *United States v. Westley James Keyes*, 1:22-mj-00009-SJB (W.D.M.I) January 11, 2022) (Continuation of Criminal Complaint), attached as Ex. 6, law enforcement stated that HSI received information from Australia law enforcement, Queensland Police Service (QPS) Child Abuse & Sexual Crime Group Task Force ARGOS—the same unit that the FBI worked with to investigate Benjamin Faulkner and Patrick Falte, two individuals associated with the investigation of the purported creator of the target website in this case, Tyler Walker—about child abuse images shared on Tor, as part of the "Queensland Police Service['s] active[] investigate[on of] darknet boards that are known to be dedicated to the proliferation of child exploitation material." *Id.* at ¶¶ 4-5. As in other cases stemming from this same operation, the

foreign law enforcement agency provided U.S. law enforcement with user-specific content from the website, including copies of "chat messages it obtained from different dark web boards posted by" a particular user." *Id.* at ¶ 19.

These four new cases further support Mr. Sanders's arguments in support of his Motions to Compel, Motions to Suppress, and Motion for a New Trial, including that the investigation of the target website in this case was part of a joint operation between U.S. law enforcement and FLAs, that NITs were used to generate such a large number of IP address leads, that U.S. law enforcement understood that the FLA's tip with respect to Mr. Sanders meant only that he had visited the target website on one date, at one time, and that there is significant information material to Mr. Sanders's motions to compel and motions to suppress that the government has withheld from this Court and the defense. *See also* Updated Case Comparison, attached as Ex. 7.

Respectfully submitted,

/s/
Jonathan Jeffress (#42884)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: jchong-smith@kaiserdillon.com

/s/
Nina J. Ginsberg (#19472)
DiMuroGinsberg, P.C.
1101 King Street, Suite 610
Alexandria, VA 22314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
Email: nginsberg@dimuro.com

/s/
H. Louis Sirkin (admitted *pro hac vice*)
Santen & Hughes
600 Vine Street, Suite 2700
Cincinnati, OH 45202
Telephone: (513) 721-4450
Facsimile: (513) 721-0109
Email: hls@santenhughes.com

Counsel for Defendant Zackary Ellis Sanders

CERTIFICATE OF SERVICE

I hereby certify that on this 22nd day of March 2022, the foregoing was served electronically on the counsel of record through the US District Court for the Eastern District of Virginia Electronic Document Filing System (ECF) and the document is available on the ECF system.

/s/ Jonathan Jeffress
Jonathan Jeffress

Exhibit 1

FILED
DEC - 8 2020
CLERK, U.S. DISTRICT COURT
NORFOLK, VA

AFFIDAVIT IN SUPPORT OF APPLICATION FOR ISSUANCE OF A CRIMINAL COMPLAINT

I, David J. Desy, being first duly sworn state:

1. I have been employed as a Special Agent ("SA") of the FBI since 2004, and am currently assigned to the Norfolk Division. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training in forensic software/hardware, child/adolescent interviewing, computer design and networking, computer intrusion investigations, asset forfeiture, informant development, surveillance, case management, victim advocacy and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography (CP)[1] (as defined in 18 U.S.C. § 2256(8)) and child exploitation (CE), and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also received training and conducted investigations involving multiple peer-to-peer (P2P) networks, the Darkweb, The Onion Router (TOR), another other online methods of distributing and receiving CP. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. I have conducted an investigation of the offenses described in this affidavit. As a result of my investigation, information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals, I am familiar with the circumstances of this on-going investigation. I have not included each and every fact known to me in this affidavit, but only the facts I believe are necessary to establish probable cause to believe THOMAS JOSEPH HOLMSTEDT has engaged in the crime of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B).

PERTINENT FEDERAL CRIMINAL STATUTES

4. 18 U.S.C. § 2252(a)(4)(B) prohibits any person from knowingly possessing, or attempting to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the

[1] I use the terms "child pornography" and "visual depictions/images of minors engaging in sexually explicit conduct" interchangeably in this Affidavit.

DJD

production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

PROBABLE CAUSE TO ARREST THOMAS JOSEPH HOLMSTEDT

5. In August 2019, a foreign law enforcement agency notified the FBI that on April 13, 2019, a user of IP address 70.160.151.223 ("the Target IP Address") accessed images of minors engaging in sexually explicit conduct via a website. The website at issue was an online bulletin board on the The Onion Router ("Tor") network dedicated to the advertisement and distribution of child pornography that operated from approximately 2016 to June 2019. On the site's announcements page was the following text: "this website was created to host videos, photos and discussions of 18 (twinks) and younger of Hurtcore materials (videos & pictures) as well as discussion of such." Hurtcore refers to violent pornography.

6. The Tor network is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network. The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network. Unlike standard Internet websites, a Tor-based web address is comprised of a series of at least 16 and as many as 56 algorithm-generated characters, followed by the suffix ".onion."

7. An administrative subpoena issued to Cox Communications on or about September 11, 2019, regarding the Target IP Address identified the account holder as Thomas Holmstedt, with an account active since 2005 at an address in Virginia Beach, Virginia ("the Virginia Beach residence").

8. On June 23, 2020, the Honorable United States Magistrate Judge Douglas E. Miller of the United States District Court for the Eastern District of Virginia authorized the installation and use of a pen register/trap and trace ("PRTT") device to record, decode and/or capture all dialing, routing addressing and signaling information associated with each communication to or from the Target IP Address. Analysis of the data provided pursuant to that PRTT order revealed evidence that a user of the internet at the Virginia Beach residence regularly accessed the Tor network, over a total of 200 times, beginning June 26, 2020, and continuing through August 21, 2020.

9. On August 21, 2020, the Honorable United States Magistrate Judge Lawrence R. Leonard of the United States District Court for the Eastern District of Virginia authorized a search warrant for the Virginia Beach residence. On August 25, 2020, agents from the FBI executed the search warrant. HOLMSTEDT and his wife were present and identified as the only full-time residents of the Virginia Beach residence. HOLMSTEDT refused to discuss anything regarding child pornography. After voluntarily signing an advice of rights form, he stated that all electronic devices in the residence were his. HOLMSTEDT also stated that he was familiar with The Live Amnesic Incognito Live System ("TAILS"), an operating system that preserves anonymity by routing internet traffic through Tor.

10. The TAILS operating system and artifacts of TAILS and Tor use were found on several devices in HOLMSTEDT's residence, including on an HP laptop computer in his bedroom closet registered to "TJ" (a match to HOLMSTEDT's first and middle names). Further, a SanDisk MicroSD card found in a dresser drawer in HOLMSTEDT's bedroom contained the TAILS operating system and a text file entitled "Simple links." That text file contained a number of bookmarked website links to Tor sites known to contain and file-share images of minors engaging in SEC. Many titles for the bookmarks contained express references to minors, such as "Baby," "chinese girls," and "loli."

11. Forensic review of electronic devices seized during the execution of the search warrant revealed two electronic devices containing visual depictions of minors engaging in SEC. First, a wireless 1 Terabyte Western Digital external hard drive, manufactured outside of the Commonwealth of Virginia and found in the hallway of HOLMSTEDT's residence, contained 128 such images, all of which depict an adult male inserting a tampon into the anus of a female infant. These images were found in the thumbnail cache. The thumbnail cache is created when a larger image file is viewed as a thumbnail by a computer user.

12. Second, a 400 Gigabyte SanDisk MicroSD card manufactured outside of the Commonwealth of Virginia and found in a desk drawer in the spare bedroom that THOMAS HOLMSTEDT's adult son, Rachid Holmstedt,[2] occasionally uses. The MicroSD card 739 images and two videos depicting minors engaging in SEC. All of the images depict a female child between eight and ten years old performing oral sex on an adult male's penis. One video involves a prepubescent female child between four and seven years old having a n adult male's penis ejaculate in her mouth and on her face. All of these files were found in slack space, indicating that they had been deleted but not yet overwritten.

13. The Internet is an interconnected network of computers with which one communicates when online, is a network that crosses state and national borders, and is a means and facility of interstate and foreign commerce.

14. Virginia Beach is in the Eastern District of Virginia.

15. On December 7, 2020, the affiant was notified by Virginia Beach Police Department ("VBPD") that THOMAS HOLMSTEDT was taken into custody after VBPD received a complaint from his son, Rachid Holmstedt, who was concerned that THOMAS HOLMSTEDT was suicidal. VBPD reported the following to the affiant: VBPD encountered THOMAS HOLMSTEDT at a dock in Rudee Inlet. He identified that he was a target of a federal investigation and had planned to commit suicide that day. HOLMSTEDT had chartered a fishing boat under the pretense of scattering the ashes of a loved one out at sea, and the captain and first-mate of the boat agreed to give HOLMSTEDT privacy at the back of the boat while they were out at sea. HOLMSTEDT purchased a .38 Special pistol and brought weights with

[2] Rachid Holmstedt was called to the Virginia Beach residence during the execution of the search warrant. He informed law enforcement that he resided at the Virginia Beach residence about half the time, but that due to COVID-19 exposure concerns, he had not been at the residence at all between August 14, 2020 and August 21, 2020, during which time the PRTT analysis noted regular Tor activity at the Virginia Beach residence.

him, planning to shoot himself in the head, fall overboard and the weights would help his body sink. When taken into custody, HOLMSTEDT had on his person the pistol, the weights, anti-anxiety medication, $1,000 cash, and three sealed letters he had written to his son, to law enforcement, and to the U.S. Coast Guard. HOLMSTEDT was taken into custody and is scheduled to be sent to a psychiatric center for a 72-hour evaluation.

CONCLUSION

16. Based on the information and evidence set forth above, I respectfully submit that there is probable cause to believe that THOMAS JOSEPH HOLMSTEDT, on or about August 25, 2020, knowingly possessed matter which contained a visual depiction that had been mailed, and had been shipped and transported using a means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce, and which was produced using materials which have been mailed and so shipped and transported, by any means including by computer, and the producing of such visual depiction involved the use of a minor engaging in sexually explicit conduct, and such visual depiction was of such conduct, and at least one visual depiction depicted a prepubescent minor and a minor who had not attained 12 years of age.

17. Accordingly, I request that a complaint be issued charging THOMAS JOSEPH HOLMSTEDT with such offenses.

FURTHER AFFIANT SAYETH NOT.

Special Agent David J. Desy
Federal Bureau of Investigation

SUBSCRIBED and SWORN before me on this 8th of December 2020 by telephone.

UNITED STATES MAGISTRATE JUDGE

Exhibit 2

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Norfolk Division

FILED
IN OPEN COURT
FEB 4 2021
CLERK, U.S. DISTRICT COURT
NORFOLK, VA

UNITED STATES OF AMERICA

v.

THOMAS JOSEPH HOLMSTEDT,

Defendant.

No. 2:21-cr-4

STATEMENT OF FACTS

The United States and the defendant, THOMAS JOSEPH HOLMSTEDT (hereinafter, "the defendant"), agree that at trial, the United States would have proven the following facts beyond a reasonable doubt with admissible and credible evidence:

1. In August 2019, a foreign law enforcement agency notified the Federal Bureau of Investigation ("FBI") that on April 13, 2019, a user of IP address 70.160.151.223 ("the Target IP address") accessed online child sexual abuse and exploitation material on the Internet via a website. The website at issue was an online bulletin board on The Onion Router ("Tor") network dedicated to the advertisement and distribution of visual depictions of minors engaging in sexually explicit conduct that operated from approximately 2016 to June 2019. On the site's announcements page was the following text: "this website was created to host videos, photos and discussions of 18 (twinks) and younger of Hurtcore materials (videos & pictures) as well as discussion of such." Hurtcore refers to violent pornography.

2. Sections and forums for posting to the website included "HURTCORE Toddlers Videos (Ages 0-5)," "Preteen/Hebe Children Videos (Ages 6-13)," "Teens Videos (Ages 14+)," "Toddlers Images (Ages 0-5)," "Preteen/Hebe Children Images (Ages 6-13)," and "Teens Images

(Ages 14+)." Another forum was named "GORE/DEATH" which included sub-forms for "Toddlers (Ages 0-5)," "Preteen/Hebe Children (Ages 6-13)" and "Teens (Ages 14+)."

3. The Tor network is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network. The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network. Unlike standard Internet websites, a Tor-based web address is comprised of a series of at least 16 and as many as 56 algorithm-generated characters, followed by the suffix ".onion."

4. An administrative subpoena issued to Cox Communications on or about September 11, 2019, regarding the Target IP address identified the account holder as Thomas Holmstedt, with an account active since 2005 at an address in Virginia Beach, Virginia ("the Virginia Beach residence").

5. On June 23rd, 2020, the U.S. District Court for the Eastern District of Virginia authorized the installation and use of a pen register/trap and trace ("PRTT") device to record, decode and/or capture all dialing, routing addressing and signaling information associated with each communication to or from the Target IP address. Analysis of the data provided pursuant to that PRTT order revealed evidence that a user of the Internet at the Virginia Beach residence regularly accessed the Tor network, over a total of 200 times, beginning June 26, 2020, and continuing through August 21, 2020.

6. On August 25, 2020, agents from the FBI executed a search warrant at the Virginia Beach residence. After voluntarily signing an advice of rights form, the defendant stated that all electronic devices in the residence were his. He also stated that he was familiar with The Live

Amnesic Incognito Live System ("TAILS"), an operating system that preserves anonymity by routing internet traffic through Tor.

7. The TAILS operating system and artifacts of TAILS and Tor use were found on several devices in the defendant's residence, including on an HP laptop computer in his bedroom closet registered to "TJ" (a match to the defendant's first and middle names). Further, a SanDisk MicroSD card found in a dresser drawer in the defendant's bedroom contained the TAILS operating system and an encrypted text file entitled "Simple links." That text file contained a number of bookmarked links to Tor sites known to contain and file-share visual depictions of minors engaging in sexually explicit conduct. Many titles for the bookmarks contained express references to minors, such as "Baby," "chinese girls," and "loli."

8. Forensic review of electronic devices seized during the execution of the search warrant at the Virginia Beach residence revealed two electronic devices containing visual depictions of minors engaging in sexually explicit conduct. First, a wireless 1 Terabyte Western Digital external hard drive, manufactured outside of the Commonwealth of Virginia and found in the hallway of the defendant's residence, contained 133 such images. 128 of these images depict an adult male inserting a tampon into the anus of a female infant. An example of one such image is the filename ending in "35ab5.jpg". These images were found in the thumbnail cache; a thumbnail is generated when an image file is viewed as a thumbnail by a computer user.

9. Second, a 400 Gigabyte SanDisk manufactured outside of the Commonwealth of Virginia and found in a desk drawer in the spare bedroom of the Virginia Beach residence, contained at least 739 images and at least two videos depicting minors engaging in sexually explicit conduct. All of the 739 images depict a female child between eight and ten years old performing oral sex on an adult male's penis. An example of one such image is the filename ending in

"0825_Carved.jpg". One of the two videos involves a prepubescent female child between four and seven years old having an adult male's penis ejaculate in her mouth and on her face. This video has the filename ending in "015_Carved.mp4". All of these files were found in slack space, indicating that they had been deleted but not yet overwritten.

10. The Internet is an interconnected network of computers with which one communicates when on-line, is a network that crosses state and national borders, and is a means and facility of interstate and foreign commerce.

11. Virginia Beach is in the Eastern District of Virginia.

12. The investigation and evidence revealed that on or about August 25, 2020, in Virginia Beach, within the Eastern District of Virginia, and elsewhere, the defendant, THOMAS JOSEPH HOLMSTEDT, did knowingly possess matter, namely a 1 Terabyte Western Digital external hard drive, which was manufactured outside the Commonwealth of Virginia, and which contained a visual depiction that had been mailed, and had been shipped and transported using a means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce, and which was produced using materials which have been mailed and so shipped and transported, by any means including by computer, and the producing of such visual depiction involved the use of a minor engaging in sexually explicit conduct, and such visual depiction was of such conduct, and at least one visual depiction depicted a prepubescent minor and a minor who had not attained 12 years of age, an example of which being a file identified by the file name ending with "35ab5.jpg".

13. This statement of facts includes those facts necessary to support the plea agreement between the defendant and the United States. It does not include each and every fact known to

the defendant or to the United States, and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

14. The actions of the defendant, as recounted above, were in all respects knowing and deliberate, and were not committed by mistake, accident, or other innocent reason.

Respectfully submitted,

Raj Parekh
Acting United States Attorney

Date: February 4, 2021

By: _____
E. Rebecca Gantt
Assistant United States Attorney

After consulting with my attorney and pursuant to the plea agreement entered into this day between the defendant, THOMAS JOSEPH HOLMSTEDT, and the United States, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

THOMAS JOSEPH HOLMSTEDT

I am Noah Weisberg, defendant's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Noah Weisberg, Esq.
Attorney for THOMAS JOSEPH HOLMSTEDT

AO 245B (Rev. 09/19) (VAE 01/22) Judgment in a Criminal Case
Sheet 1

UNITED STATES DISTRICT COURT
Eastern District of Virginia
Alexandria Division

UNITED STATES OF AMERICA)
)
v.)
)
ZACKARY ELLIS SANDERS,)
)
)
)

JUDGMENT IN A CRIMINAL CASE

Case Number: 1:20-cr-00143-TSE-1

USM Number: 94249-083

Jonathan Jeffress, Nina Ginsberg, Mark Mahoney, Henry Sirkin, Christopher Amolsch
Defendant's Attorney

The defendant was found guilty on Counts 1-5, 6-11 and Count 12 after a plea of not guilty.

The defendant is adjudged guilty of these offenses:

Title and Section	Nature of Offense	Offense Ended	Count
18 U.S.C. § 2251(a) and (e)	Production of Child Pornography	11/25/2019	1
18 U.S.C. § 2251(a) and (e)	Production of Child Pornography	11/14/2019	2
18 U.S.C. § 2251(a) and (e)	Production of Child Pornography	04/14/2018	3
18 U.S.C. § 2251(a) and (e)	Production of Child Pornography	12/11/2017	4
18 U.S.C. § 2251(a) and (e)	Production of Child Pornography	10/21/2017	5
18 U.S.C. § 2252(a)(2) and (b)(1)	Receipt of Child Pornography	01/16/2020	6
18 U.S.C. § 2252(a)(2) and (b)(1)	Receipt of Child Pornography	11/25/2019	7
18 U.S.C. § 2252(a)(2) and (b)(1)	Receipt of Child Pornography	11/14/2019	8
18 U.S.C. § 2252(a)(2) and (b)(1)	Receipt of Child Pornography	04/14/2018	9
18 U.S.C. § 2252(a)(2) and (b)(1)	Receipt of Child Pornography	12/11/2017	10
18 U.S.C. § 2252(a)(2) and (b)(1)	Receipt of Child Pornography	10/21/2017	11
18 U.S.C. § 2252(a)(4)(B) and (b)(2)	Possession of Child Pornography	02/2020	12

The defendant is sentenced as provided in pages 2 through 10 of this Judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States attorney of material changes in economic circumstances.

/s/
T. S. Ellis, III
United States District Judge

April 1, 2022
Date of Imposition of Judgment

April 1, 2022
Date

Case Number: 1:20-cr-00143-TSE-1
Defendant's Name: SANDERS, ZACKARY ELLIS

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a term of TWO HUNDRED AND SIXTEEN (216) MONTHS with credit for time served as computed by the Bureau of Prisons pursuant to statute.

This term of imprisonment consists of terms of TWO HUNDRED AND SIXTEEN (216) MONTHS on each of Counts 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 and 11 to run concurrently with each other and ONE HUNDRED AND TWENTY (120) MONTHS on Count 12 to run concurrently with the sentences imposed on Count 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 and 11.

The Court makes the following recommendations to the Bureau of Prisons:

1. The Court recommends that the defendant be housed at the Alexandria Detention Center in Alexandria, Virginia and not be removed until the Bureau of Prisons designates a specific facility where the defendant will be transported directly to serve his sentence.

   The Court further notes that the defendant hired an expert to assess, based on defendant's various medical conditions and need for sex offender treatment, to what facility defendant should be designated. Defendant's expert recommends that defendant be designated to FCI Butner Low in North Carolina.

   Defendant has a number of medical conditions and ADC and BOP should be careful and alert to make sure he receives treatment for his medical conditions.

2. The Court furthermore recommends that the defendant's medication, Kesimpta, be administered as prescribed by the defendant's doctors.

The court makes the following recommendations to the Bureau of Prisons:

☒ The defendant is remanded to the custody of the United States Marshal.

RETURN

I have executed this judgment as follows: _____

Defendant delivered on _____ to _____
at _____, with a certified copy of this Judgment.

_____
UNITED STATES MARSHAL

By _____
DEPUTY UNITED STATES MARSHAL

Case Number: 1:20-cr-00143-TSE-1
Defendant's Name: SANDERS, ZACKARY ELLIS

SUPERVISED RELEASE

Upon release from imprisonment, you will be on supervised release for a LIFETIME TERM.

This term consists of terms of LIFETIME TERM on each of Counts 1, 2, 3, 4 and 5 and FIVE (5) YEARS on each of Counts 6, 7, 8, 9, 10, 11 and 12 to run concurrently with each other.

MANDATORY CONDITIONS

1. You must not commit another federal, state or local crime.
2. You must not unlawfully possess a controlled substance.
3. You must refrain from any unlawful use of a controlled substance. You must submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.
   ☐ The above drug testing condition is suspended, based on the court's determination that you pose a low risk of future substance abuse. *(check if applicable)*
4. ☒ You must make restitution in accordance with 18 U.S.C. §§ 3663 and 3663A or any other statute authorizing a sentence of restitution. *(check if applicable)*
5. ☐ You must cooperate in the collection of DNA as directed by the probation officer. *(check if applicable)*
6. ☒ You must comply with the requirements of the Sex Offender Registration and Notification Act (34 U.S.C. § 20901, et seq.) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in the location where you reside, work, are a student, or were convicted of a qualifying offense. *(check if applicable)*
7. ☐ You must participate in an approved program for domestic violence. *(check if applicable)*

You must comply with the standard conditions that have been adopted by this court as well as with any other conditions on the attached page.

Case Number: 1:20-cr-00143-TSE-1
Defendant's Name: SANDERS, ZACKARY ELLIS

STANDARD CONDITIONS OF SUPERVISION

As part of your supervised release, you must comply with the following standard conditions of supervision. These conditions are imposed because they establish the basic expectations for your behavior while on supervision and identify the minimum tools needed by probation officers to keep informed, report to the court about, and bring about improvements in your conduct and condition.

1. You must report to the probation office in the federal judicial district where you are authorized to reside within 72 hours of your release from imprisonment, unless the probation officer instructs you to report to a different probation office or within a different time frame.
2. After initially reporting to the probation office, you will receive instructions from the court or the probation officer about how and when you must report to the probation officer, and you must report to the probation officer as instructed.
3. You must not knowingly leave the federal judicial district where you are authorized to reside without first getting permission from the court or the probation officer.
4. You must answer truthfully the questions asked by your probation officer.
5. You must live at a place approved by the probation officer. If you plan to change where you live or anything about your living arrangements (such as the people you live with), you must notify the probation officer at least 10 days before the change. If notifying the probation officer in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.
6. You must allow the probation officer to visit you at any time at your home or elsewhere, and you must permit the probation officer to take any items prohibited by the conditions of your supervision that he or she observes in plain view.
7. You must work full time (at least 30 hours per week) at a lawful type of employment, unless the probation officer excuses you from doing so. If you do not have full-time employment you must try to find full-time employment, unless the probation officer excuses you from doing so. If you plan to change where you work or anything about your work (such as your position or your job responsibilities), you must notify the probation officer at least 10 days before the change. If notifying the probation officer at least 10 days in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.
8. You must not communicate or interact with someone you know is engaged in criminal activity. If you know someone has been convicted of a felony, you must not knowingly communicate or interact with that person without first getting the permission of the probation officer.
9. If you are arrested or questioned by a law enforcement officer, you must notify the probation officer within 72 hours.
10. You must not own, possess, or have access to a firearm, ammunition, destructive device, or dangerous weapon (i.e., anything that was designed, or was modified for, the specific purpose of causing bodily injury or death to another person such as nunchakus or tasers).
11. You must not act or make any agreement with a law enforcement agency to act as a confidential human source or informant without first getting the permission of the court.
12. If the probation officer determines that you pose a risk to another person (including an organization), the probation officer may require you to notify the person about the risk and you must comply with that instruction. The probation officer may contact the person and confirm that you have notified the person about the risk.
13. You must follow the instructions of the probation officer related to the conditions of supervision.

U.S. Probation Office Use Only

A U.S. probation officer has instructed me on the conditions specified by the court and has provided me with a written copy of this judgment containing these conditions. For further information regarding these conditions, see *Overview of Probation and Supervised Release Conditions*, available at: www.uscourts.gov

Defendant's Signature _____ Date

Case Number: 1:20-cr-00143-TSE-1
Defendant's Name: SANDERS, ZACKARY ELLIS

SPECIAL CONDITIONS OF SUPERVISION

1) The defendant shall pay restitution totaling at least **$6,000**. $3000 each to "Andy" who is depicted in the "Spongebob" series and John Doe IV who is depicted in the "8 Kids" series. Restitution shall be payable immediately, and each restitution payment shall be divided proportionately among the victims.

   If not paid in full by the time he is released from custody, any remaining balance on the court-ordered financial obligations shall be paid at a rate of no less than **$100 per month**, to begin within **60 days** of release.

2) Pursuant to the Adam Walsh Child Protection and Safety Act of 2006, the defendant shall register with the state sex offender registration agency in any state where the defendant resides, works, and attends school, according to federal and state law and as directed by the probation officer.

3) Pursuant to the Adam Walsh Child Protection and Safety Act of 2006, the defendant shall submit to a search of his person, property, house, residence, vehicle, papers, computer, other electronic communication or data storage devices or media, and effects at any time, by any law enforcement or probation officer with reasonable suspicion concerning unlawful conduct or a violation of a condition of supervision, upon prior notification to and approval by the court or with a warrant.

4) The defendant shall participate in a program approved by the United States Probation Office for mental health treatment, to include a psychosexual evaluation and sex offender treatment. The costs of these programs are to be paid by the defendant as directed by the probation officer. The defendant shall waive all rights of confidentiality regarding sex offender/mental health treatment to allow the release of information to the United States Probation Office and authorize communication between the probation officer and the treatment provider.

5) The defendant shall submit to any testing or assessments required as part of his sexual offender therapeutic treatment. The costs of the testing are to be paid by the defendant, as directed by the probation officer.

6) The defendant shall not engage in employment or volunteer services that allow him access to computers or minors.

7) The defendant shall not purchase, possess or view any sexually explicit material or images using young juvenile models under the age of 18 in any format including, but not limited to, in magazines, books, on the computer, or any electronic device, in videos, movies, and television.

8) The defendant shall have no contact with minors unless supervised by a competent, informed adult, approved in advance by the probation officer.

9) The defendant shall not utilize any sex-related adult telephone services, websites, or electronic bulletin boards. The defendant shall submit any records requested by the probation officer to verify compliance with this condition including, but not limited to, credit card bills, telephone bills, and cable/satellite television bills.

10) The defendant shall pay a total **of $60,000** special assessment pursuant to 18 U.S.C. § 3014, based on future earnings ability with penalties and interest waived.

11) Pursuant to 18 U.S.C. § 2259A(a)(3), beginning on the date of enactment of the Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018, the Court shall assess an amount of up to $50,0000. Accordingly, the Courts finds the defendant indigent and imposes a **zero** amount as it pertains to Counts 1 through 12 of the Indictment.

Case Number: 1:20-cr-00143-TSE-1
Defendant's Name: SANDERS, ZACKARY ELLIS

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

	Assessment	Restitution	Fine	AVAA Assessment*	JVTA Assessment**
TOTALS	$ 1,200.00	$ 6,000.00	$ 0.00	$ 0.00	$ 60,000.00

☐ The determination of restitution is deferred until _____. An *Amended Judgment in a Criminal Case (AO 245C)* will be entered after such determination.

☒ The defendant must make restitution (including community restitution) to the following payees in the amount listed in the Restitution ordered by the Court on April 1, 2022.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all nonfederal victims must be paid before the United States is paid.

☒ Restitution amount ordered by the Court on April 1, 2022 $ 6,000.00

The restitution shall be in the sum of $3000 each to "Andy" who is depicted in the "Spongebob" series and John Doe IV who is depicted in the "8 Kids" series.

☐ The defendant must pay interest on restitution and a fine of more than $2,500, unless the restitution or fine is paid in full before the fifteenth day after the date of the judgment, pursuant to 18 U.S.C. § 3612(f). All of the payment options on Sheet 6 may be subject to penalties for delinquency and default, pursuant to 18 U.S.C. § 3612(g).

☒ The court determined that the defendant does not have the ability to pay interest and it is ordered that:

☒ the interest requirement is waived for the ☐ fine ☒ restitution and JVTA Assessment.

☐ the interest requirement for the ☐ fine ☐ restitution is modified as follows:

* Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018, Pub. L. No. 115-299.
** Justice for Victims of Trafficking Act of 2015, Pub. L. No. 114-22.
*** Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

AO 245B (Rev. 09/19) (VAE 11/21) Judgment in a Criminal Case
Sheet 6 – Schedule of Payments

Case Number: 1:20-cr-00143-TSE-1
Defendant's Name: SANDERS, ZACKARY ELLIS

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

A ☒ Lump sum payment of $66,000 due immediately, balance due
- ☐ not later than _____ , or
- ☒ in accordance with ☐ C, ☒ D, ☐ E, or ☐ F below; or

B ☒ Payment to begin immediately (may be combined with ☐ C, ☒ D, or ☐ F below); or

C ☐ Payment in equal *(e.g., weekly, monthly, quarterly)* installments of $ over a period of *(e.g., months or years)*, to commence *(e.g., 30 or 60 days)* after the date of this judgment; or

D ☒ Payment in equal *monthly* installments of $100, to commence *60 days* after release from imprisonment to a term of supervision; or

E ☐ Payment during the term of supervised release will commence within *(e.g., 30 or 60 days)* after release from imprisonment. The court will set the payment plan based on an assessment of the defendant's ability to pay at that time; or

F ☒ Special instructions regarding the payment of criminal monetary penalties:

1) Pursuant to 18 U.S.C. § 3014, the defendant is ordered to pay a special assessment in the amount of $60,000 with penalties and interest waived.

2) Pursuant to 18 U.S.C. § 2259A(a)(3), beginning on the date of enactment of the Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018, the Court shall assess an amount of up to $50,000. Accordingly, the Court finds the defendant indigent and imposes a zero amount on each of Counts 1 through 12 of the Indictment.

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during the period of imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

☐ Joint and Several

☐ The defendant shall pay the cost of prosecution.

☐ The defendant shall pay the following court cost(s):

☒ The defendant shall forfeit the defendant's interest in the following property to the United States:
Pursuant to Fed. R. Crim. P. 32.2(b), the Court must enter an order of forfeiture. Forfeiture to be determined at a later date.

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) AVAA assessment, (5) fine principal, (6) fine interest, (7) community restitution, (8) JVTA assessment, (9) penalties, and (10) costs, including cost of prosecution and court costs.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	Case No. 1:20-CR-143
v.	)	
	)	Honorable T.S. Ellis, III
ZACKARY ELLIS SANDERS,	)	
	)	
Defendant.	)	
	)	

UNITED STATES' NOTICE OF FILING OF REDACTED MEMORANDUM OPINION AND PROPOSED RESTITUTION ORDER

The United States of America, by and through undersigned counsel, respectfully submits this notice of filing of a redacted version of the Court's Sealed Memorandum Opinion (ECF No. 615) and a proposed Restitution Order for the Court's consideration and, in support thereof, states as follows:

1. On March 31, 2022, the Court issued a Sealed Memorandum Opinion (ECF No. 615) and a non-sealed Order (ECF No. 616). In its Order, the Court directed the parties to "meet and confer regarding what redactions, if any at all, are necessary to the Sealed Memorandum Opinion so that a public version may be filed" and to "submit any proposed redactions on or before Friday, April 8, 2022." ECF No. 616.

2. Attached to this filing as Exhibit 1 is a copy of the Court's Sealed Memorandum Opinion with a limited number of proposed redactions consistent with the prior redactions to the Court's publicly filed rulings. *See* ECF No. 122. Because the Court's Memorandum Opinion is currently under seal, the version with proposed redactions will be filed under seal directly with the Clerk's Office. The United States submits that these limited redactions are necessary to protect sensitive information that is subject to the Protective Order in this case, and that protecting this

sensitive information outweighs any competing interest in the public's right of access to it. ECF No. 28.

3. The United States provided a copy of the Court's Sealed Memorandum Opinion with the proposed redactions to counsel for the defendant on April 7, 2022, and sought the defendant's views on whether any additional redactions are necessary. On April 8, 2022, counsel for the defendant informed the government that the defendant "objects to all of the government's proposed redactions for the reasons previously set forth in Mr. Sanders's Opposition to the Government's Motion for Order to Show Cause and to Seal (ECF No. 184)." The defendant, however, has sought to redact similar information in the past pursuant to the Protective Order. *See, e.g.*, ECF No. 594.

4. The United States also respectfully notes that the reference to "Operation Pacifier" on page eight of the Court's Memorandum Opinion appears to be in error. "Operation Pacifier" is a prior investigation of a different website that is unrelated to this case. The United States respectfully submits that the Memorandum Opinion appears to have intended to state that two FLAs "were investigating [the Target Website, redacted]," not that they "were involved in Operation Pacifier".

5. Finally, attached to this filing as Exhibit 2 is a proposed Restitution Order for the Court's consideration. The proposed Restitution Order follows with the Court's oral imposition of restitution at the sentencing hearing on April 1, 2022. *See* ECF No. 620. The United States provided a copy of the proposed Restitution Order to counsel for the defendant on April 5, 2022.

Respectfully submitted,

Jessica D. Aber
United States Attorney

By: /s/

William G. Clayman
Special Assistant United States Attorney (LT)
Jay V. Prabhu
Seth M. Schlessinger
Assistant United States Attorneys
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700

CERTIFICATE OF SERVICE

I hereby certify that on April 8, 2022, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of that electronic filling (NEF) to counsel of record.

By: /s/

William G. Clayman
Special Assistant United States Attorney (LT)
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
Email: william.g.clayman@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant.	Case No. 1:20-cr-00143 Honorable T.S. Ellis, III

ZACKARY ELLIS SANDERS'S NOTICE OF APPEAL

Notice is hereby given that Defendant Zackary Ellis Sanders appeals to the United States Court of Appeals for the Fourth Circuit from the Final Judgment (Dkt. 621) entered against him in this action on April 1, 2022, and all decisions and orders subsidiary thereto and subsumed therein.

Dated: April 13, 2022

Respectfully submitted,

/s/

Jonathan Jeffress (#42884)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: jchong-smith@kaiserdillon.com

/s/
Nina J. Ginsberg (#19472)
DiMuroGinsberg, P.C.
1101 King Street, Suite 610
Alexandria, VA 22314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
Email: nginsberg@dimuro.com

/s/
H. Louis Sirkin (admitted *pro hac vice*)
Santen & Hughes
600 Vine Street, Suite 2700
Cincinnati, OH 45202
Telephone: (513) 721-4450
Facsimile: (513) 721-0109
Email: hls@santenhughes.com
Counsel for Defendant Zackary Ellis Sanders

CERTIFICATE OF SERVICE

I hereby certify that on this 13th day of April 2022, the foregoing was served electronically on the counsel of record through the US District Court for the Eastern District of Virginia Electronic Document Filing System (ECF) and the document is available on the ECF system.

/s/ Jonathan Jeffress
Jonathan Jeffress

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Interview of:
Zackary Ellis Sanders

Conducted By:

SA Christopher Ford
SA Jeremy Obie

Date of Interview: February 12, 2020

Audio Transcription

Diversified Reporting Services, Inc.
1426 Duke Street
Alexandria, Virginia 22314
Phone: 202-467-9208
Fax: 202-293-1254

GOVERNMENT
EXHIBIT
102A
1:20-CR-143

[redacted]

SPECIAL AGENT OBIE: What kind of applications do you think are best to communicate with these days? Like, do you have a certain amount of applications? Like, Mobile apps, something like that? Like --

MR. SANDERS: I mean, Facebook. I text message, like I'm, you know --

SPECIAL AGENT OBIE: You don't have any, any other like, like WhatsApp, Wickr, Telegram, anything like

that?

MR. SANDERS: I've got Telegram.

SPECIAL AGENT OBIE: Okay. What is Telegram? Like, it's, it's like a mobile messaging something, right, or --

MR. SANDERS: Yeah. It's like an -- it's like, it's like texting or iMessage sort of, but like there's some groups on Telegram. So you're going to be like a, like -- I mean, I guess it's like a group chat on whatever, but you know, you can --

SPECIAL AGENT OBIE: Like, what do you do, like you share pictures? Videos? Just communicate via text? Like, how does it work, like --

MR. SANDERS: Yeah. I mean, I don't really send -- I don't send any photos or anything. I mean, like the group -- I'm only, I'm in like a handful of groups, but most of them are like, LGBT, like gay, you know, there's two like, DC area groups. Part of a D.C. area, kind of friends group on there.

So you know, it's people like, you know, "What are you doing today?" "What are you doing today?" and then you know --

SPECIAL AGENT OBIE: Yeah.

MR. SANDERS: -- some people send photos of themselves. I don't really send any photos, because I just

-- I don't really take photos of myself, so -- but --

SPECIAL AGENT OBIE: Yeah. I understand.

MR. SANDERS: Some people alone take them of themselves, it's --

SPECIAL AGENT FORD: That's probably smart, so --

MR. SANDERS: Yeah.

SPECIAL AGENT FORD: -- you don't end up --

MR. SANDERS: I know, yeah.

SPECIAL AGENT OBIE: Is that, is that like -- I know some apps are like, encrypted, or whatever, like, are those like, in an encrypted or --

MR. SANDERS: No.

SPECIAL AGENT OBIE: -- just, just regular chats?

MR. SANDERS: I think there's like a way to encrypt Telegram. I don't, I don't know.

SPECIAL AGENT OBIE: Okay.

SPECIAL AGENT FORD: What's your -- do you have a -- so --

SPECIAL AGENT OBIE: Isn't it called like a handle or like a profile --

SPECIAL AGENT FORD: Yeah.

SPECIAL AGENT OBIE: -- or like what, what is it?

MR. SANDERS: I think just like a username.

SPECIAL AGENT OBIE: Username? Well, well --

MR. SANDERS: Or maybe it's a -- I don't, I don't

know. When it's -- or when you set it up, it's like, I had to type in a name and whatever.

SPECIAL AGENT OBIE: Uh-huh. What's your name on there?

MR. SANDERS: I don't remember.

SPECIAL AGENT OBIE: When's the last time you accessed it?

MR. SANDERS: I mean, I had to open a group -- one of my groups yesterday, but -- I mean, it doesn't like, say what my name is, it just --

SPECIAL AGENT OBIE: Uh-huh.

MR. SANDERS: -- but -- because like, there's like the actual username that's like your -- like if you search for someone, the name, but then --

SPECIAL AGENT FORD: That's your display name.

MR. SANDERS: -- just a -- but just like the display name is --

SPECIAL AGENT OBIE: Yeah, yeah.

MR. SANDERS: -- is, different. So like, I know my display name.

SPECIAL AGENT OBIE: What's the display name?

MR. SANDERS: I mean, it's like, SirZack.

SPECIAL AGENT OBIE: SirZack.

SPECIAL AGENT FORD: Hmm. Fancy. What about any other apps that you have?

SPECIAL AGENT OBIE: Like WhatsApp, Kik, what are the other apps?

SPECIAL AGENT FORD: Snapchat?

SPECIAL AGENT OBIE: Snapchat --

SPECIAL AGENT FORD: Instagram?

SPECIAL AGENT OBIE: -- Instagram --

MR. SANDERS: Got Snapchat. I have Instagram but I don't use Instagram. Like, I've wanted to -- like for my business, I have --

SPECIAL AGENT FORD: Yeah.

MR. SANDERS: -- a Instagram page, but I've never been like, great at taking photos.

SPECIAL AGENT FORD: See this, this camera and this phone, man, it's --

MR. SANDERS: Yeah.

SPECIAL AGENT FORD: -- some magical -- is that the -- is this the newest one?

MR. SANDERS: No. That -- I need to get a new one.

SPECIAL AGENT FORD: Okay.

MR. SANDERS: But --

SPECIAL AGENT FORD: Which one is this?

MR. SANDERS: That's a iPhone X.

SPECIAL AGENT FORD: X, okay. I think -- I don't know, I don't, I don't know which one I have.

MR. SANDERS: They came out like two-and-a-half years ago.

SPECIAL AGENT FORD: Okay.

MR. SANDERS: And it was like, it was the first one that didn't have a home button on it, and everyone went crazy about it.

SPECIAL AGENT FORD: Oh. He's a, he's a -- he's a Android user, so he doesn't understand --

MR. SANDERS: Okay.

SPECIAL AGENT FORD: -- the struggles of --

MR. SANDERS: You're, you're against me.

SPECIAL AGENT FORD: But just have -- that having the button, because I just got this phone.

MR. SANDERS: Yeah.

SPECIAL AGENT FORD: And not having the button has -- I'm like, always hitting here --

MR. SANDERS: [Inaudible -- simultaneous discussion] --

SPECIAL AGENT FORD: -- I'm like, "Oh," like, "there's no button there."

MR. SANDERS: Same, yeah. The most annoying is like, with no headphone jack on the --

SPECIAL AGENT FORD: Oh, my goodness.

SPECIAL AGENT OBIE: See?

SPECIAL AGENT FORD: Got to put the little

extension --

MR. SANDERS: Because no one, no one carries the adapter when they need it and then -- yeah.

SPECIAL AGENT FORD: That's the worst thing.

SPECIAL AGENT OBIE: Just switch to Android.

SPECIAL AGENT FORD: Yeah, because you always have earphones on you, but the adapter --

MR. SANDERS: All right, to be fair, when I first was getting like a -- like a real smart phone, I -- there was apps that I wanted that weren't available on Android at the time. They are now, but --

SPECIAL AGENT FORD: Zack, you don't, you don't have to apologize for being a, for being a Apple user.

MR. SANDERS: -- so it's like --

SPECIAL AGENT FORD: It's okay.

SPECIAL AGENT OBIE: You need to apologize for being an Apple --

MR. SANDERS: There's a reason --

SPECIAL AGENT FORD: It's okay, we, we -- I know we're like a cult, but it's okay. It's all right, you're fine. All right.

[redacted]

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Interview of:
Zackary Ellis Sanders

Conducted By:

SA Christopher Ford
SA Jeremy Obie

Date of Interview: February 12, 2020

Audio Transcription

Diversified Reporting Services, Inc.
1426 Duke Street
Alexandria, Virginia 22314
Phone: 202-467-9208
Fax: 202-293-1254

GOVERNMENT
EXHIBIT
103A
1:20-CR-143

[redacted]

SPECIAL AGENT OBIE: So is that where -- how many, how many files or devices do you think are on the -- that flash drive? Estimate.

MR. SANDERS: [Pause] I'm, I'm not sure. Let me -- can I, I just get to the Tor stuff, is that --

SPECIAL AGENT FORD: Yeah. We'll go back to it.

MR. SANDERS: It paints a clearer picture.

SPECIAL AGENT FORD: Gotcha.

MR. SANDERS: So like I saw some of that and I guess didn't really know what to make of it, but then at some point was kind of -- I don't know how to explain it.

[redacted]

SPECIAL AGENT OBIE: Just explain it. We've heard everything, we've seen everything.

MR. SANDERS: No, but I guess I -- I'm trying to figure out how even I felt.

SPECIAL AGENT FORD: So let's go back, let's go back to, let's go back to the Wiki page, the Tor Wiki page.

MR. SANDERS: Okay. So --

SPECIAL AGENT OBIE: Where'd you go from there? What did you click on?

MR. SANDERS: There was a point in which I looked at -- I was, you know, clicking around links. And then kind of one took me to like a site that had like some child pornography on it.

SPECIAL AGENT OBIE: What site was that? Do you remember?

MR. SANDERS: [Pause] Well first it was like a pop up of some like, just random pictures that I didn't click on. Like, it just kind of popped up while I was on a different site on Tor. Because I was, I was literally just like -- the first time I was on there, I was just like, "What is this site?" Like a -- I've seen a -- you know, and then some things popped up.

And then I kind of, I think, ended up clicking on something. And then it took me to like, to some child pornography. I think the site was called -- it was like,

something like, "Boy Videos." It was like, "Boy Vids 4" I think --

SPECIAL AGENT OBIE: Okay.

MR. SANDERS: -- is what it was. And kind of looked around a bit. And then a while ago I think I -- when I clicked on a link there it downloaded some to like, my computer.

SPECIAL AGENT FORD: Go back to that.

SPECIAL AGENT OBIE: What do you mean you think it --

SPECIAL AGENT FORD: Yeah. Did you -- you didn't download it, it just happened --

MR. SANDERS: If I -- there was like a title of something and I clicked on it, and it's like -- and then when you, when you clicked on it, it like popped up with a -- like a download box.

SPECIAL AGENT FORD: Right. And then you have to, you have to do another action. You have to save it. You can do either save or cancel. So you, you hit save --

MR. SANDERS: I think I hit just enter on the keyboard.

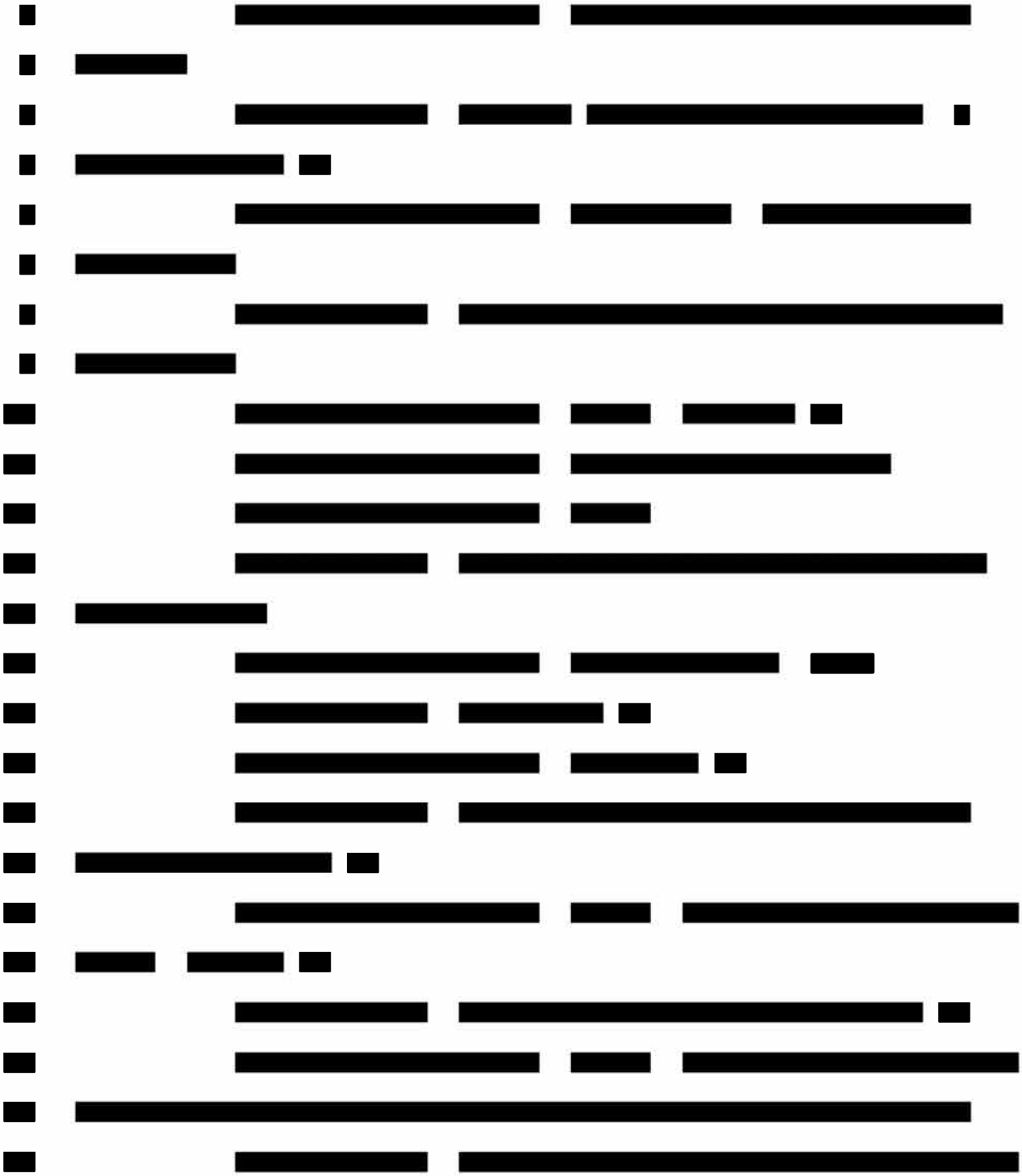
SPECIAL AGENT FORD: Okay.

MR. SANDERS: So like it, it downloaded --

SPECIAL AGENT FORD: Mm-hmm.

MR. SANDERS: -- you know, like a -- it was like

a file that had like, multiple files in it.



IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Interview of:
Zackary Ellis Sanders

Conducted By:

SA Christopher Ford
SA Jeremy Obie

Date of Interview: February 12, 2020

Audio Transcription

Diversified Reporting Services, Inc.
1426 Duke Street
Alexandria, Virginia 22314
Phone: 202-467-9208
Fax: 202-293-1254

GOVERNMENT
EXHIBIT
104A
1:20-CR-143

[redacted]

SPECIAL AGENT FORD: All right, so we can keep, keep the thing moving. All right. Is there anything anywhere else you would go to get child porn or was that the -- it just -- Tor? So even in like, Telegram, Kik -- oop, God -- Telegram, Kik -- sorry, if I fall it is what it is. So Telegram, Kik, and like, none of those sites you would get in groups where they're sending child porn?

MR. SANDERS: So at that -- as I said, like when I was younger there was a group or somebody sent on --

SPECIAL AGENT FORD: Talking about -- I'm talking about today.

MR. SANDERS: -- on Kik, many years ago.

SPECIAL AGENT FORD: Talking about right now. If

I -- now if -- when I go into your phone --

MR. SANDERS: I have not seen any today. I have not seen any yesterday.

SPECIAL AGENT FORD: Okay.

MR. SANDERS: I -- you know --

SPECIAL AGENT OBIE: So you mentioned that you, you went into your -- that flash drive.

MR. SANDERS: Well I moved everything on there, like a -- for like a --

SPECIAL AGENT OBIE: Right. Like, so the last time you went in there to --

MR. SANDERS: Weeks -- yeah.

SPECIAL AGENT OBIE: -- look at it was within this month.

MR. SANDERS: No.

SPECIAL AGENT OBIE: Or within a month's timeframe.

MR. SANDERS: It might have been a little before. But some -- somewhat around there is when I --

SPECIAL AGENT OBIE: Okay.

MR. SANDERS: -- pulled everything that was left on the laptop off, to my knowledge, and put it onto the flash drive.

[redacted]

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Interview of:
Zackary Ellis Sanders

Conducted By:

SA Christopher Ford
SA Jeremy Obie

Date of Interview: February 12, 2020

Audio Transcription

GOVERNMENT
EXHIBIT
105A
1:20-CR-143

Diversified Reporting Services, Inc.
1426 Duke Street
Alexandria, Virginia 22314
Phone: 202-467-9208
Fax: 202-293-1254

[redacted]

MR. SANDERS: In fact, like, I mean I -- since you have that flash drive, I mean --

SPECIAL AGENT FORD: Yeah, I --

MR. SANDERS: -- I guess you're going to see what's on it. The -- I'm just going to say like, I don't like some of things that are on there.

SPECIAL AGENT FORD: Okay.

MR. SANDERS: Some files that are on there, it's like, when I downloaded something it came in like a, like a package almost.

SPECIAL AGENT FORD: Mm-hmm. Like a zip file?

MR. SANDERS: Yeah.

SPECIAL AGENT FORD: Got it.

MR. SANDERS: So there's some things there that

like, are really like, disgusting to me.

SPECIAL AGENT FORD: Yeah.

MR. SANDERS: I mean, all -- okay.

SPECIAL AGENT OBIE: Just speak.

MR. SANDERS: Some -- okay. I don't want this to sound bad on the, on the recording. But like, if someone's like, 16 or something, I mean, that's the age of consent in several states, like --

SPECIAL AGENT FORD: Mm-hmm. It's still a kid, but go ahead.

SPECIAL AGENT OBIE: Just speak freely.

SPECIAL AGENT FORD: Yeah.

SPECIAL AGENT OBIE: Right?

SPECIAL AGENT FORD: Mm-hmm.

MR. SANDERS: You know, like in many states it would be legal to do something with -- not saying it's right or wrong --

SPECIAL AGENT OBIE: Right.

MR. SANDERS: -- I'm just saying like, that's very different to a degree in my mind than like --

SPECIAL AGENT FORD: Like tiny tots.

MR. SANDERS: Like a tiny -- yeah.

SPECIAL AGENT FORD: Yes. Yeah.

MR. SANDERS: I think that, that like in some of those like, zip files, there may have been some like,

younger, so -- which I really don't like and --

SPECIAL AGENT FORD: Yeah.

MR. SANDERS: -- like don't want. But it like, it's part of the zip files.

SPECIAL AGENT FORD: It's part of the, the -- that's not what you were looking for, but it's part of the package.

MR. SANDERS: Exactly.

SPECIAL AGENT FORD: Makes sense.

MR. SANDERS: So it's like, not what I'd ever go after.

SPECIAL AGENT FORD: Got it.

MR. SANDERS: But like, it just came with it and like, wouldn't necessarily know it was part of that until it downloaded.

SPECIAL AGENT OBIE: So when you like, extracted the zip file --

MR. SANDERS: Mm-hmm.

SPECIAL AGENT OBIE: -- to get the actual -- get to the actual content, would you download that to your laptop and then put it to that -- your speed drive or what?

MR. SANDERS: Download and unzip.

SPECIAL AGENT OBIE: Like what, what -- where, where would the content go? Would it be on this computer and then you put it in your --

MR. SANDERS: For a little while it was on here.

SPECIAL AGENT OBIE: Okay.

MR. SANDERS: And then I wanted to kind of just be done with all of it --

SPECIAL AGENT FORD: Mm-hmm.

MR. SANDERS: -- after a while. And then I just put it on a flash drive, moved it all onto there, wiped it off the computer, kind of deleted everything -- files. Sanitized the computer and --

SPECIAL AGENT FORD: Did you, did you go on Tor to get this -- the child porn? Like it's kind of hard for me to believe that somebody stumbles upon this stuff on Tor because it's very -- I wouldn't say it's very sophisticated, but people go on Tor because they don't want to be found.

MR. SANDERS: Mm-hmm.

SPECIAL AGENT FORD: And, and I know -- and I know through years of doing this --

MR. SANDERS: Yeah.

SPECIAL AGENT FORD: -- that maybe in some groups, they're like, they'll say, "Hey, go to this site on Tor because it has fresh content," or "It has this." It's -- it's very hard for me to believe -- and I want to believe you.

MR. SANDERS: Okay.

SPECIAL AGENT FORD: But it's very hard for me to believe that you just stumbled upon this.

SPECIAL AGENT OBIE: Particularly because you said you previously got child porn on Kik.

MR. SANDERS: Yeah. So like when I was younger, like I was sent something on, on Kik and like, saw things on Kik. And then -- I don't want to use the word like interest, but like --

SPECIAL AGENT FORD: Curious?

MR. SANDERS: -- you know, so then I like went to Tor to like, look at it.

SPECIAL AGENT FORD: Mm-hmm.

SPECIAL AGENT OBIE: Okay.

MR. SANDERS: I mean, the first time I was on Tor I was just -- the very first time I was on Tor I was just like, looking just around Tor, like what Tor did. Then like, a little later, I was like, you know, "Well I wonder if this is there?" And kind -- and after I'd seen it, I kind of went, you know, looked at something.

SPECIAL AGENT FORD: Yeah.

MR. SANDERS: And then, you know, like generally stay off of it. But like, every like, occasional so often, kind --

SPECIAL AGENT FORD: You'd go on there.

MR. SANDERS: -- of just like, see what is -- was

going on.

SPECIAL AGENT FORD: That's, that's fine.

MR. SANDERS: But like I don't --

SPECIAL AGENT FORD: Have you ever, have you ever uploaded anything to --

MR. SANDERS: Never.

SPECIAL AGENT FORD: So I know there's certain sites on Topic Links that you have to --

SPECIAL AGENT OBIE: You have to --

SPECIAL AGENT FORD: -- in order to get access to the group to the --

MR. SANDERS: Never.

SPECIAL AGENT FORD: -- closed content --

MR. SANDERS: I would never look -- I'd go -- if I click on one of those sites and I saw that, I'd be like, "No." Because I never wanted this to happen.

SPECIAL AGENT FORD: Yeah, but why -- but before I, before I joined the FBI --

MR. SANDERS: Yeah.

SPECIAL AGENT FORD: -- I knew nothing about like, if I upload something this could happen. So --

MR. SANDERS: Well because I saw like, on one of the sites, like, people were talking about like, I guess like, protecting your computer, whatever.

SPECIAL AGENT FORD: Mm-hmm.

MR. SANDERS: I don't -- I didn't really do anything, but I guess -- you know, I just didn't want to upload anything, because it's like, I didn't want to be part of it, but like I was curious to see some of it.

[redacted]

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Interview of:
Zackary Ellis Sanders

Conducted By:

SA Christopher Ford
SA Jeremy Obie

Date of Interview: February 12, 2020

Audio Transcription

GOVERNMENT
EXHIBIT
106A
1:20-CR-143

Diversified Reporting Services, Inc.
1426 Duke Street
Alexandria, Virginia 22314
Phone: 202-467-9208
Fax: 202-293-1254

[redacted]

SPECIAL AGENT FORD: So I want you just to -- this is your opportunity to just let it out and this way you leave it to us to -- for -- you leave it on us to do the more investigation part. I just need your -- I just want your word --

MR. SANDERS: Yeah.

SPECIAL AGENT FORD: -- and your word only. I don't want --

MR. SANDERS: No, I'm trying to -- I'm truly trying to think, I'm not trying to hide anything.

SPECIAL AGENT FORD: Okay. I know you're -- and, and it's a lot.

MR. SANDERS: Yeah.

SPECIAL AGENT FORD: I mean, we knock on your door at six in the morning, you had just fell asleep. And I'm very happy you're not the guy that I -- we find kids in a basement, locked up. Like, that, that would have made, made me very upset. It would have been a very bad day.

MR. SANDERS: Yeah.

SPECIAL AGENT FORD: But --

SPECIAL AGENT OBIE: First case.

SPECIAL AGENT FORD: -- but you are --

MR. SANDERS: I almost wish that is what you found so you could put an end to that.

SPECIAL AGENT FORD: No -- yeah, right.

MR. SANDERS: But you know, I hear you -- I -- yeah, I, I, I getcha.

SPECIAL AGENT FORD: Right.

MR. SANDERS: Yeah.

SPECIAL AGENT FORD: So and I, and I don't feel like that's -- you're that type of guy. But I -- people, people do things and that's why we're here, we're --

MR. SANDERS: I, I understand.

SPECIAL AGENT FORD: We're, you know, we're here to get your side of it so I can go back, I can be like, "Okay, look, Zack just made a mistake. It is what it is and" -- "but he's not the guy that we're looking for. Those, those guys that are doing that stuff."

MR. SANDERS: I, I understand. Yeah.

SPECIAL AGENT FORD: So I want to get your -- I want to -- and I don't think that you've been untruthful to us, but I just -- just don't hold back because you're trying to protect somebody else or -- like, at the end we're going to, we're going to find what we're looking for.

MR. SANDERS: I, I literally have no one to protect.

SPECIAL AGENT FORD: Okay.

MR. SANDERS: There's, there's -- there's nothing. I -- I've, I've never sent anything. I mean, even on, even on like an app. Like, if I'll have like an underage person message me --

SPECIAL AGENT FORD: Mm-hmm.

MR. SANDERS: -- like occasionally like on, like a dating app or something, you know, they go on there. Like, and they would like, send me a dick pick. I'm like, "No." Like, I won't even do that.

SPECIAL AGENT FORD: Good.

MR. SANDERS: Because I'm like, you're -- like I, like, would I meet with you for coffee? Maybe, you know, if --

SPECIAL AGENT FORD: Right.

MR. SANDERS: -- you're like 17, you know, 18, you know, whatever, sure. I'm like, I, I did not send any nudes. Like, I don't, I don't want from you -- you know --

SPECIAL AGENT FORD: All right.

MR. SANDERS: Because -- no.

[redacted]


7850
GOVERNMENT
EXHIBIT
201
1:20-CR-143


A
GOVERNMENT
EXHIBIT
202
1:20-CR-143

GOVERNMENT
EXHIBIT
203
1:20-CR-143


GOVERNMENT
EXHIBIT
204
1:20-CR-143
S


V
GOVERNMENT
EXHIBIT
205
1:20-CR-143


V
GOVERNMENT
EXHIBIT
206
1:20-CR-143


GOVERNMENT
EXHIBIT
207
1:20-CR-143

Total Pages:(467 of 494)
USCA4 Appeal: 22-4242 Doc: 14-3 Filed: 06/16/2022 Pg: 467 of 494

GOVERNMENT
EXHIBIT
208
1:20-CR-143




GOVERNMENT
EXHIBIT
209
1:20-CR-143



USCA4 Appeal: 22-4242 Doc: 14-3 Filed: 06/16/2022 Pg: 469 of 494
Total Pages:(469 of 494)


GOVERNMENT
EXHIBIT
211
1:20-CR-143

GOVERNMENT
EXHIBIT
212
1:20-CR-143

GOVERNMENT EXHIBIT 213 1:20-CR-143



GOVERNMENT EXHIBIT
214
1:20-CR-143





GOVERNMENT
EXHIBIT
215
1:20-CR-143

USCA4 Appeal: 22-4242 Doc: 14-3 Filed: 06/16/2022 Pg: 474 of 494
Total Pages:(474 of 494)
JA1351

Total Pages:(475 of 494)
Pg: 475 of 494
Filed: 06/16/2022
Doc: 14-3
USCA4 Appeal: 22-4242

02 . 12 . 2020 06 : 45

GOVERNMENT
EXHIBIT
216
1:20-CR-143

Where Restaurants Shop®

ALL OF OUR PAPER PRODUCTS ARE TRUE DAILY TRUE PACK

Buy or Lease One Clover Solution, Get One FREE!* Up to $4,000* in Savings

Call Today! 1-866-478-7554

MID-ATLANTIC/NJ • OCTOBER 2019

JA1352


GOVERNMENT
EXHIBIT
217
1:20-CR-143
02 . 12 . 2020 06 : 57


EliteBook 755
GOVERNMENT
EXHIBIT
218
1:20-CR-143
02 . 12 . 2020 06 : 57


GOVERNMENT
EXHIBIT
219
1:20-CR-143
02 . 12 . 2020 06 : 59


iPad
GOVERNMENT
EXHIBIT
220
1:20-CR-143
02 . 12 . 2020 07 : 01

iPad

Designed by Apple in California Assembled in China Model A1709
FCC ID: BCGA1709 IC: 579C-A1709 Serial: DMPVGGCPHPDV

GOVERNMENT
EXHIBIT
221
1:20-CR-143

02 . 12 . 2020 07 : 02



GOVERNMENT
EXHIBIT
222
1:20-CR-143

02 . 12 . 2020 07 : 22



GOVERNMENT EXHIBIT 223 1:20-CR-143


LIFESAVERS GUMMIES
Starburst
TIMEX
GOVERNMENT EXHIBIT 224 1:20-CR-143
02 . 12 . 2020 07 : 03


GOVERNMENT
EXHIBIT
225
1:20-CR-143
Farrish
CHRYSLER Jeep DODGE RAM SUBARU
Andrew Morris
Service Lane Manager
Farrish of Fairfax
9610 Fairfax Blvd
Phone: 703-934-1600
Direct: 703-934-1602
COMPAQ
VAIO
DEAD COMPUTERS
REFER A FRIEND
SanDisk
Sharpie
Stick
02 · 12 · 2020 07 : 10

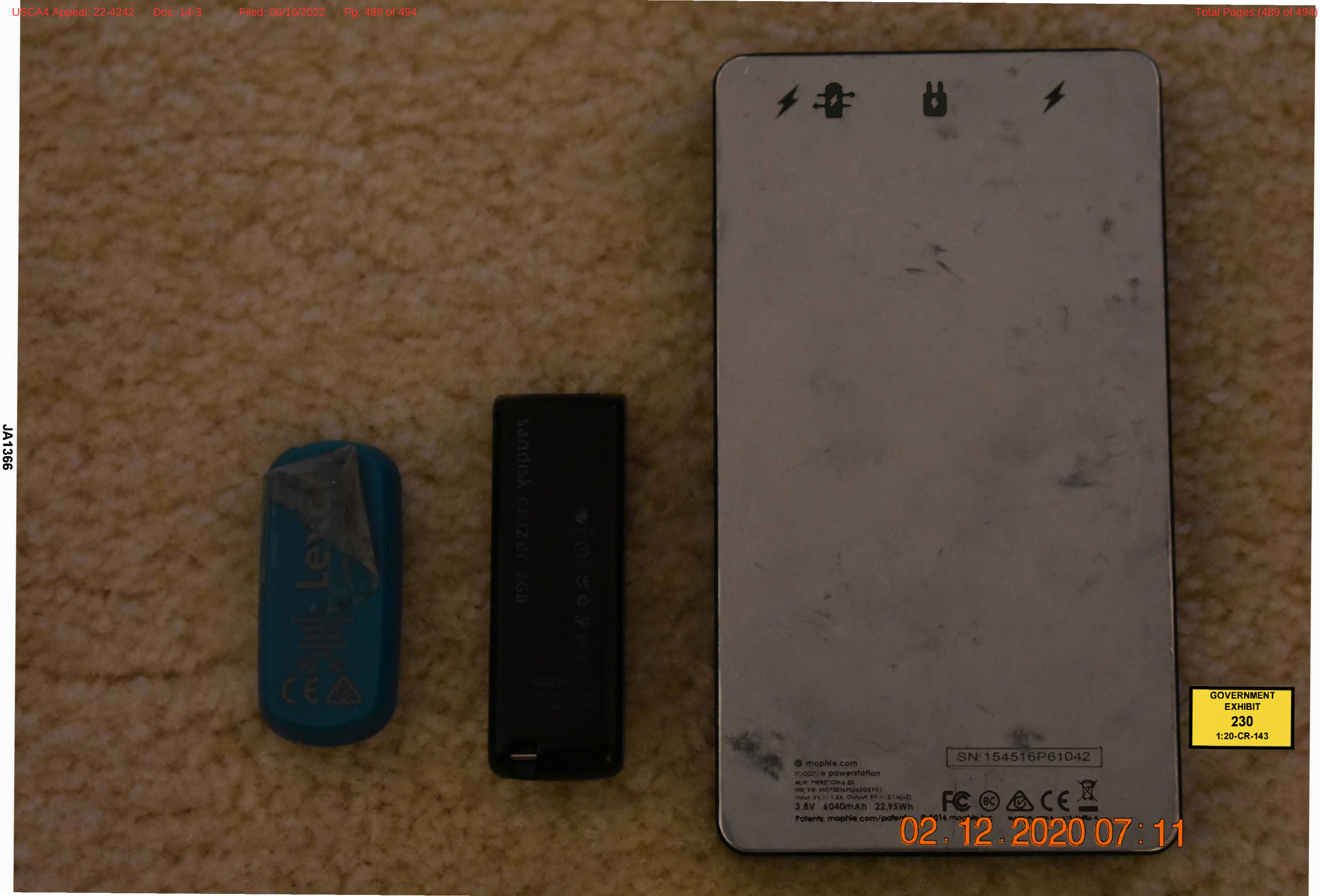

GOVERNMENT
EXHIBIT
226
1:20-CR-143
02.12.2020 07:03
CLASSIC
CHERRY
MADE IN TAIWAN
Wyeth Consumer Healthcare, Madison, NJ 07940 USA © 2009 Wyeth
For most recent
product information,
visit www.chapstick.com
ChapStick
3 0573-1905-30 4
Sun Alert:
Limiting sun exposure, wearing protective clothing, and using sunscreens may reduce the risks of skin aging, skin cancer, and other harmful effects of the sun.
Drug Facts
Active ingredients
Padimate O 1.5%
White petrolatum 44%
Purposes
Sunscreen
Skin protectant
PAA008925
Uses
helps prevent and temporarily protects chafed, chapped or cracked lips
helps prevent and protects from the drying effects of wind and cold weather
helps prevent sunburn
higher SPF gives more sunburn protection
Warnings
Stop use and ask a doctor if
rash or irritation develops and lasts
Keep out of reach of children. If swallowed, get medical help or contact a Poison Control Center right away.
Directions
apply liberally before sun exposure and as needed
children under 6 months of age: ask a doctor
Other information store at 20-25°C (68-77°F)
Inactive ingredients arachidyl propionate, camphor, carnauba wax, cetyl alcohol, D&C red no. 6 barium lake, fragrance, isopropyl linolate, isopropyl myristate, lanolin, light mineral oil, menthol, methylparaben, octyldodecanol, paraffin, phenyl trimethicone, propylparaben, saccharin, white wax
32G
Lexar


OASIS
CONCESSIONS
OASIS
CONCESSIONS
GOVERNMENT
EXHIBIT
227
1:20-CR-143
02 . 12 . 2020 07 : 10

GOVERNMENT
EXHIBIT
228
1:20-CR-143

02 . 12 . 2020 07 : 10


32G
Lexar
SN:154516P61042
GOVERNMENT
EXHIBIT
229
1:20-CR-143
02 . 12 . 2020 07 : 11



GOVERNMENT EXHIBIT 230 1:20-CR-143



USCA4 Appeal: 22-4242 Doc: 14-3 Filed: 06/16/2022 Pg: 490 of 494
Total Pages:(490 of 494)


MAGNUM
CLOSET
C
GOVERNMENT
EXHIBIT
232
1:20-CR-143

GOVERNMENT EXHIBIT 233 1:20-CR-143

GOVERNMENT EXHIBIT 234 1:20-CR-143

Numark LA C/NO. 417 MADE IN CHINA

MAGNUM STEALTH FORCE 8.0 UNIFORM US 11 EU 44 UK 10

LARGE ENOUGH TO SERVICE SMALL ENOUGH TO CARE!

02.12.2020 07:18


GOVERNMENT
EXHIBIT
235
1:20-CR-143
02 . 12 . 2020 07 : 26