

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

In re Sealed Docket Sheet Associated With Malware  
Warrant Issued on July 22, 2013

Civil Action No. \_\_\_\_\_

**MOTION TO UNSEAL COURT DOCKET SHEET**

For the reasons stated in the accompanying memorandum of law, the American Civil Liberties Union, the American Civil Liberties Union Foundation, the American Civil Liberties Union of Maryland, and the American Civil Liberties Union Foundation of Maryland respectfully move for this Court to unseal any currently sealed docket sheets associated with any search warrants issued by this Court on July 22, 2013 that authorize the surreptitious use of surveillance software (commonly referred to as “malware”) to acquire identifying information from private computers.

August 25, 2016

Respectfully submitted,

Brett Max Kaufman (*pro hac vice* to be filed)  
Nathan Freed Wessler (*pro hac vice* to be filed)  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION  
125 Broad St., 18th Floor  
New York, NY 10004  
Tel: (212) 549-2500  
Fax: (212) 549-2654  
Email: bkaufman@aclu.org



---

David Rocah (Bar No. 27315)  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION OF MARYLAND  
3600 Clipper Mill Road  
Suite 350  
Baltimore, MD 21211  
Tel: (410) 889-8550  
Fax: (410) 366-7838  
Email: rocah@aclu-md.org

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

In re Sealed Docket Sheet Associated With Malware  
Warrant Issued on July 22, 2013

Civil Action No. \_\_\_\_\_

**MEMORANDUM OF LAW IN SUPPORT OF  
MOTION TO UNSEAL COURT DOCKET SHEET**

**Table of Contents**

Introduction..... 1

Jurisdiction..... 3

Background..... 3

    I. The government’s use of malware to hack into private computers ..... 3

    II. The government’s use of malware pursuant to a warrant issued by this Court ..... 5

Standing ..... 9

Argument ..... 9

    I. The First Amendment requires unsealing the docket sheet listing the malware warrant issued in this District..... 11

        A. A constitutional right of access applies to the docket sheet listing the malware search warrant. .... 11

            1. There is a “centuries-long” tradition of access to docket sheets..... 11

            2. Logic demands keeping docket sheets open. .... 12

        B. There is no governmental interest that outweighs the public’s right of access to the malware-warrant docket sheet, and even if there were, sealing the docket sheet is not a tailored means of accommodating that interest..... 14

    II. The common law also requires unsealing the malware docket sheet. .... 16

Conclusion ..... 17

**Table of Authorities**

**Cases**

*Balt. Sun Co. v. Goetz*, 886 F.2d 60 (4th Cir. 1989)..... 11, 12

*Bernstein v. Bernstein*, No. 14 Civ. 6867, 2016 WL 1071107 (S.D.N.Y. Mar. 18, 2016)..... 12

*Doe v. Pub. Citizen*, 749 F.3d 246 (4th Cir. 2014) ..... 10, 11, 13

*FTC v. Standard Fin. Mgmt. Corp.*, 830 F.2d 404 (1st Cir. 1987)..... 13

*Globe Newspaper Co. v. Fenton*, 819 F. Supp. 89 (D. Mass. 1993) ..... 12

*Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982) ..... 9, 14

*Hartford Courant Co. v. Pellegrino*, 380 F.3d 83 (2d Cir. 2004)..... passim

*In re Application to Unseal 98 Cr. 1101 (ILG)*, 891 F. Supp. 2d 296 (E.D.N.Y. 2012) ..... 12

*In re Knight Publ’g Co.*, 743 F.2d 231 (4th Cir. 1984) ..... 9

*In re Search of Fair Fin.*, 692 F.3d 424 (6th Cir. 2012)..... 12

*In re Search Warrant for Secretarial Area Outside Office of Gunn*, 855 F.2d 569 (8th Cir. 1988)..... 10, 12, 15

*In re State-Record Co.*, 917 F.2d 129 (4th Cir. 1990) ..... 10, 11, 15, 17

*In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013)..... 2, 4

*In re Wash. Post*, 807 F.2d 383 (4th Cir. 1986)..... 9

*Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992) ..... 9

*N.Y. Civil Liberties Union v. N.Y. City Transit Auth.*, 684 F.3d 286 (2d Cir. 2011) ..... 9

*Nixon v. Warner Commc’ns, Inc.*, 435 U.S. 589 (1978)..... 3

*Oliner v. Kontrabecki*, 745 F.3d 1024 (9th Cir. 2014) ..... 16

*Perez-Guerrero v. U.S. Atty. Gen.*, 717 F.3d 1224 (11th Cir. 2013) ..... 16

*Press-Enter. Co. v. Superior Court*, 478 U.S. 1 (1986)..... 9, 10, 11

*Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555 (1980)..... 3

*Rushford v. New Yorker Magazine, Inc.*, 846 F.2d 249 (4th Cir. 1988) ..... 10

*Stone v. Univ. of Md. Med. Sys. Corp.*, 855 F.2d 178 (4th Cir. 1988)..... 10, 13, 15

*United States v. Index Newspapers, LLC*, 766 F.3d 1072 (9th Cir. 2014)..... 12

*United States v. Levin*, -- F. Supp. 3d --, No. 15 Cr. 10271, 2016 WL 2596010 (D. Mass. 2016)..... 5

*United States v. Martin*, 684 F. Supp. 341 (D. Mass. 1988)..... 15

*United States v. Matish*, -- F. Supp. 3d --, No. 16 Cr. 16, 2016 WL 3545776 (E.D. Va. 2016)..... 5

*United States v. Mendoza*, 698 F.3d 1303 (10th Cir. 2012)..... 11

*United States v. Ochoa-Vasquez*, 428 F.3d 1015 (11th Cir. 2005)..... 11

*United States v. Ring*, 47 F. Supp. 3d 38 (D.D.C. 2014) ..... 9

*United States v. Sonin*, -- F. Supp. 3d --, No. 15 Cr. 116, 2016 WL 908650 (E.D. Wis. 2016)..... 10

*United States v. Valenti*, 987 F.2d 708 (11th Cir. 1993)..... 11

*Va. Dep’t of State Police v. Wash. Post*, 386 F.3d 567 (4th Cir. 2004)..... passim

*Webster Groves Sch. Dist. v. Pulitzer Publ’g Co.*, 898 F.2d 1371 (8th Cir. 1990) ..... 11

*Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009) ..... 2

**Other Authorities**

Craig Timberg & Ellen Nakashima, *FBI’s Search for ‘Mo,’ Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, Wash. Post, Dec. 6, 2013, <http://wpo.st/FzRh1> ..... 4, 5

David Bisson, *FBI Used Metasploit Hacking Tool in ‘Operation Torpedo,’ Tripwire*, Dec. 16, 2014, <http://tripwire.me/29efAEC> ..... 5

Ellen Nakashima, *This Is How the Government Is Catching People Who Use Child Porn Sites*, Wash. Post, Jan. 21, 2016, [http://wpo.st/\\_lRh1](http://wpo.st/_lRh1) ..... 2, 6, 8

FBI, Press Release, *Brattleboro Man Sentenced to Prison for Child Pornography Offense* (Oct. 28, 2014), <http://1.usa.gov/28T3Ohq>..... 7, 15

Gregg Keizer, *FBI Planted Spyware on Teen’s PC to Trace Bomb Threats*, Computerworld, July 19, 2007, <http://www.computerworld.com/article/>

2542586/data-privacy/fbi-planted-spyware-on-teen-s-pc-to-trace-bomb-  
threats.html..... 4

*IP Address*, Dictionary.com, <http://www.dictionary.com/browse/ip-address> ..... 1

Joseph Cox, *The FBI’s ‘Unprecedented’ Hacking Campaign Targeted Over a  
Thousand Computers*, Motherboard, Jan. 5, 2016,  
[http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-  
targeted-over-a-thousand-computers](http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-<br/>targeted-over-a-thousand-computers) ..... 5

Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware  
Attack*, Wired, Sept. 13, 2013, [https://www.wired.com/2013/09/freedom-  
hosting-fbi](https://www.wired.com/2013/09/freedom-<br/>hosting-fbi)..... 6, 15

Kevin Poulsen, *FBI’s Secret Spyware Tracks Down Teen Who Made Bomb  
Threats*, Wired, July 18, 2007, <http://www.wired.com/2007/07/fbi-spyware> ..... 3, 4

Nat Hentoff, *The FBI’s Magic Lantern*, Village Voice, May 28, 2002,  
<http://www.villagevoice.com/news/the-fbis-magic-lantern-6413591> ..... 3

Sen. Ron Wyden, Rule 41 Remarks at the Open Tech. Inst., June 30, 2016,  
*available at* [https://www.wyden.senate.gov/news/press-releases/wyden-  
untested-government-mass-hacking-techniques-threaten-digital-security-  
critical-infrastructure](https://www.wyden.senate.gov/news/press-releases/wyden-<br/>untested-government-mass-hacking-techniques-threaten-digital-security-<br/>critical-infrastructure)..... 5

Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, And  
Less Than a Wiretap: What the StingRay Teaches Us About How Congress  
Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16  
Yale J.L. & Tech. 134 (2013) ..... 2

## Introduction

The American Civil Liberties Union, the American Civil Liberties Union Foundation, the American Civil Liberties Union of Maryland, and the American Civil Liberties Union Foundation of Maryland (together, the “ACLU”) respectfully move this Court to unseal any sealed docket sheets associated with any search warrants issued by this Court on July 22, 2013 that authorize the surreptitious use of surveillance software (referred to by the FBI as a “Network Investigative Technique” or “NIT” and more commonly known as “malware”) to acquire identifying information from private computers. A malware warrant issued by this Court on July 22, 2013 is referenced in an affidavit that was filed in support of an application to search the home of a suspect in *United States v. Klein*, No. 13 Mj. 00117, Doc. 1-3, at 16, ¶ 16.c (D. Vt. Nov. 20, 2013) (attached as “Exhibit C”), but no corresponding warrant appears on the public docket sheet for *United States v. Klein* (attached as “Exhibit A”), or (to the knowledge of the ACLU) on any other public docket sheet. Because the public has First Amendment and common-law rights to access them, this Court should unseal any sealed docket sheets with entries for malware warrants (and related materials) issued by the Court on July 22, 2013.

The terms “NIT” and “malware” refer to code delivered surreptitiously to one or more computers that enables the collection of private information about the user(s), including identifying information such as an IP address.<sup>1</sup> Such code is used by hackers to steal passwords and other personal information.<sup>2</sup> Increasingly, the FBI has used malware to pierce the online

---

<sup>1</sup> An IP address is “a code that identifies a computer network or a particular computer or other device on a network, consisting of four numbers separated by periods.” *IP Address*, Dictionary.com, <http://www.dictionary.com/browse/ip-address>.

<sup>2</sup> The Ninth Circuit Court of Appeals has described malware as software that “works by, for example, compromising a user’s privacy, . . . stealing identities, or spontaneously opening

anonymity and surveil the private communications of those it suspects of committing crimes. For example, the FBI has attempted to use malware to determine the identity of those who are suspected of committing bank fraud over the Internet. But malware can be used to ascertain far more than merely a user's identity: "the software has the capacity to search the computer's hard drive, random access memory, and other storage media[ and] to activate the computer's built-in camera." *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013) (order denying government application for warrant authorizing use of malware). Given, moreover, that "law enforcement agencies are placing malware on sites that might have thousands of users," many worry that "investigators may also wind up hacking and identifying the computers of law-abiding people who are seeking to remain anonymous, people who can also include political dissidents and journalists." Ellen Nakashima, *This Is How the Government Is Catching People Who Use Child Porn Sites*, Wash. Post, Jan. 21, 2016, [http://wpo.st/\\_IRh1](http://wpo.st/_IRh1) (hereinafter "Nakashima Article").

Although the FBI has used malware for approximately fifteen years, the executive branch has never sought explicit legislative authority to use this surveillance technology. Instead, agencies have sought judicial approval for the use of malware on an ad hoc basis by applying for search warrants under Rule 41 of the Federal Rules of Criminal Procedure.<sup>3</sup>

---

Internet links to unwanted websites . . . ." *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1171 (9th Cir. 2009).

<sup>3</sup> See generally Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, And Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J.L. & Tech. 134, 164 (2013) (describing a trend in which the "government seeks to accommodate the use of new and powerful surveillance technologies through aggressive interpretation of existing statutory language that neither directly authorizes nor prohibits their use").



The breadth and potency of malware as a law-enforcement tool raises concerns that can only be properly debated if legislators and the general public are aware of instances in which it is being used, the ways in which law enforcement seeks to use it, and the extent of judicial supervision. The sealing of docket sheets with warrants authorizing the use of malware prevents this critical public debate from happening, in violation of the public's right of access. *See Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 572 (1980) ("People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing."). The ACLU therefore respectfully requests that the Court order the unsealing of any docket sheets relating to the government's application for any malware warrants authorized by the Court on July 22, 2013.

### **Jurisdiction**

This Court has jurisdiction over this motion due to its inherent "supervisory power over its own records and files." *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 598 (1978).

### **Background**

#### **I. The government's use of malware to hack into private computers**

The FBI's use of digital spying technology dates back to at least as early as 1999, when a court authorized investigators to install a covert keystroke-logging device on a suspect's computer. Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, *Wired*, July 18, 2007, <http://www.wired.com/2007/07/fbi-spyware> (hereinafter "2007 Poulsen Article"). By 2002, the agency had developed a malware tool that could be delivered over the Internet to surveillance targets. *See* Nat Hentoff, *The FBI's Magic Lantern*, *Village Voice*, May 28, 2002, <http://www.villagevoice.com/news/the-fbis-magic-lantern-6413591>. But it was not until 2007 that an actual use of malware by the FBI was publicly revealed; the case involved a

teenager who had made bomb threats to his high school. 2007 Poulsen Article. The malware that infected the suspect's computer was used to determine the computer's IP address, log its browsing behavior, and register the IP address of every computer to which it connected.<sup>4</sup> *Id.*

In April 2013, the FBI applied for a warrant authorizing the use of malware targeting a computer belonging to individuals suspected of committing bank fraud and identity theft. *See In re Warrant*, 958 F. Supp. 2d at 755. The malware sought to be deployed could collect massive amounts of information from the targeted computer, such as browsing history, saved passwords, and email and chat communications. *Id.* at 755–56. The FBI also intended to use the targeted computer's built-in camera to take surreptitious photos of the individuals who used it. *Id.* at 759–61; *see also* Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, Wash. Post, Dec. 6, 2013, <http://wpo.st/FzRh1> (hereinafter "Timberg & Nakashima Article") (noting that, according to former FBI official, the agency had "been able to covertly activate a computer's camera—without triggering the light that lets users know it is recording—for several years"). In a public order, a federal magistrate judge denied the application, finding that the search would violate both Rule 41(b) of the Federal Rules of Criminal Procedure and the Fourth Amendment. *In re Warrant*, 958 F. Supp. 2d at 756–61.

Although the exact number is unclear, the FBI has since deployed malware of differing capabilities in numerous cases. *See* Timberg & Nakashima Article. Marcus Thomas, former assistant director of the FBI's Operational Technology Division, which contains the FBI unit

---

<sup>4</sup> Importantly, the public appears to have learned of its deployment from an FBI affidavit filed in support of a search warrant application. *See* Gregg Keizer, *FBI Planted Spyware on Teen's PC to Trace Bomb Threats*, Computerworld, July 19, 2007, <http://www.computerworld.com/article/2542586/data-privacy/fbi-planted-spyware-on-teen-s-pc-to-trace-bomb-threats.html>.

responsible for the agency's use of malware, has stated that the FBI's malware technology continues to advance and that law enforcement agencies are realizing "that they're going to have to use these types of tools more and more." *Id.*

In addition to the tailored use of malware against individual targets, the FBI has, since 2012, engaged in a number mass-hacking operations targeting thousands of individuals by delivering malware to every computer that visits a particular website under the FBI's control. David Bisson, *FBI Used Metasploit Hacking Tool in 'Operation Torpedo,'* Tripwire, Dec. 16, 2014, <http://tripwire.me/29efAEC>; Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers,* Motherboard, Jan. 5, 2016, <http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers>. These controversial hacking operations have been criticized by Members of Congress from both parties, *see, e.g.,* Sen. Ron Wyden, Rule 41 Remarks at the Open Tech. Inst., June 30, 2016, *available at* <https://www.wyden.senate.gov/news/press-releases/wyden-untested-government-mass-hacking-techniques-threaten-digital-security-critical-infrastructure>, and numerous federal courts to have considered the legality of the mass hacking warrants have ruled that such warrants violate Rule 41 of the Federal Rules of Criminal Procedure. *See, e.g., United States v. Levin*, -- F. Supp. 3d --, No. 15 Cr. 10271, 2016 WL 2596010 (D. Mass. 2016); *see also United States v. Matish*, -- F. Supp. 3d --, No. 16 Cr. 16, 2016 WL 3545776, at \*17 (E.D. Va. 2016) (collecting cases).

II. The government's use of malware pursuant to a warrant issued by this Court

In July 2013, the FBI seized a group of servers that hosted various websites on the "dark web"—a part of the Internet that cannot be accessed using ordinary search engines. Some, but not all, of the content hosted on these servers—known collectively as the "Freedom Hosting

Network”—was child pornography. Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired, Sept. 13, 2013, <https://www.wired.com/2013/09/freedom-hosting-fbi> (hereinafter “2013 Poulsen Article”).

Among the websites and services on the Freedom Hosting Network was an email service known as “TorMail,” which was “used by a range of people, from criminals to dissidents and journalists.” Nakashima Article. On August 4, 2013, the homepage of TorMail was, without warning, replaced with a “down for maintenance” message. *Id.* A number of technically sophisticated users noticed that when they visited the TorMail homepage, the website attempted to covertly deliver malware to their computers. 2013 Poulsen Article. Security researchers who subsequently analyzed the code determined that it collected identifying information about visitors to the site and then transmitted that information back to a server in Northern Virginia. The FBI later confirmed that it had deployed malware on Freedom Hosting websites after seizing the Freedom Hosting servers. *Id.*; *see also* Nakashima Article.

On November 20, 2013, the FBI applied in the District of Vermont for a warrant to search the home of Grant L. Klein. *See United States v. Klein*, No. 13 Mj. 00117, Doc. 1 (D. Vt. Nov. 20, 2013) (warrant application, attached as “Exhibit B”). The affidavit supporting the warrant application, submitted by FBI Special Agent Jeffrey W. Alford (the “Alford Affidavit”), indicates that Klein was suspected of visiting an unnamed website during the summer of 2013 that hosted images depicting child sexual exploitation. Alford Aff. ¶ 17.

Agents were aware of this website because “data from the computer server hosting [the website had been] obtained” by the FBI, but anonymity-protecting software prevented the FBI from determining the IP addresses of the website’s visitors. *Id.* ¶ 16.b. In order to learn the identities of these visitors, the FBI obtained a warrant from this Court on July 22, 2013 that

authorized the deployment of malware on the website to infect its visitors' computers. *Id.* ¶ 16.c. Between July 31 and August 5, 2013, the FBI used this malware to “identify the computer[s], [their] location[s], other information about the computer[s], and the user[s] of the computer[s] accessing” the website. *Id.*

Using this malware, the FBI determined that on August 4, 2013, a computer used by Klein visited the website and accessed child pornography. *Id.* ¶ 17.a–b. Klein was subsequently convicted of one count of possession of child pornography and sentenced to twelve years of imprisonment and ten years of supervised release. *See* FBI, Press Release, *Brattleboro Man Sentenced to Prison for Child Pornography Offense* (Oct. 28, 2014), <http://1.usa.gov/28T3Ohq> (hereinafter “Klein Press Release”).

While the July 22, 2013 warrant authorizing the use of the malware that led the FBI to identify Klein is referenced in paragraph 16 of the Alford Affidavit, the warrant itself has not been entered on the District of Vermont docket sheet associated with the search warrant for Klein's home and it is (as far as the ACLU can tell) not posted on any public docket sheet in this District, where it was issued. The potentially relevant docket may be one of the four sealed cases initiated on July 22, 2013 and assigned to magistrate judges in this District,<sup>5</sup> or it may be some other docket.

As indicated in the Alford Affidavit, the malware deployed against Klein was used to identify numerous individuals who visited a website that hosted child pornography. Alford Aff. ¶ 16.c. Beyond that, the extent of the malware's deployment is unknown. It is unclear, for instance, how many individuals' computers were infected, in which Districts, and what

---

<sup>5</sup> The case numbers for these docket sheets are: 13-mj-1553, 13-mj-1554, 13-mj-1567, and 13-mj-1749.

information was obtained. Given that the malware deployed against Klein was delivered to Freedom Hosting website visitors between July 31 and August 5, 2013, and that the TorMail malware was delivered on August 4, there is reason to believe that the website Klein visited was part of the Freedom Hosting Network, and that the malware warrant issued by this Court on July 22, 2013 was the source of authority for the deployment of malware not just against Klein, but across Freedom Hosting websites and services—which had thousands of users—including against innocent users of TorMail.

To date, the only publicly accessible warrants authorizing the FBI to engage in bulk hacking have targeted websites that are dedicated to the distribution of child pornography, and, as a result, the government has been able to assert probable cause that everyone visiting the sites is engaged in a crime. The TorMail website, in contrast, was not dedicated to the distribution of child pornography—it was a free, anonymous email service that had many users who were using it to protect their lawful private communications. Nakashima Article. That the FBI engaged in a bulk hacking operation against all visitors to TorMail, which had many lawful, valid uses, raises serious concerns about the appropriateness of bulk hacking, and the extents to which courts should be authorizing and supervising such operations.

The sealing of the docket sheet associated with the July 22, 2013 warrant prevents these concerns from being aired and debated publicly. Indeed, it prevents the public from learning or confirming even the most basic facts about the deployment of malware for law-enforcement purposes: the fact of judicial approval is unconfirmed; any reasoning supporting such approval is inaccessible; even the reasons for precluding public access are themselves inaccessible. The sealing therefore violates the public's rights under the First Amendment and the common law to access information about the activities of the executive branch and the judicial processes that

authorize them. Any sealed docket sheets relating to the malware warrant issued by this Court on July 22, 2013 should therefore be unsealed.

### **Standing**

“Members of the public have standing to move to unseal criminal proceedings.” *United States v. Ring*, 47 F. Supp. 3d 38, 41 (D.D.C. 2014) (citing *Press-Enter. Co. v. Superior Court*, 478 U.S. 1 (1986) (“*Press-Enterprise I*”)); see also *In re Knight Publ’g Co.*, 743 F.2d 231, 234 (4th Cir. 1984) (“[R]epresentatives of the press and general public ‘must be given an opportunity to be heard on the question of their exclusion.’” (quoting *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982))). The ACLU has standing to bring this public-access motion because it has suffered an injury-in-fact that is fairly traceable to the sealed docket sheet associated with the malware warrant issued by this Court on July 22, 2013. See *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992); see also *N.Y. Civil Liberties Union v. N.Y. City Transit Auth.*, 684 F.3d 286, 294–95 (2d Cir. 2011) (finding civil liberties organization had standing to challenge public’s exclusion from Transit Adjudication Bureau hearings); *In re Wash. Post*, 807 F.2d 383, 388 n.4 (4th Cir. 1986) (finding newspaper had standing to move to unseal plea hearing transcripts because “it ha[d] suffered an injury that [wa]s likely to be redressed by a favorable decision” (alteration and quotation marks omitted)).

### **Argument**

“The right of public access to documents or materials filed in a district court derives from two independent sources: the common law and the First Amendment.” *Va. Dep’t of State Police v. Wash. Post*, 386 F.3d 567, 575 (4th Cir. 2004). A First Amendment right to access judicial records attaches when the “experience and logic” test is satisfied—that is, when a record has historically been available to the public and when “public access plays a significant positive role

in the functioning of the particular process.” *Press-Enterprise II*, 478 U.S. at 8–9. When the right attaches, it “may be overcome only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest.” *Id.* at 9.

The common-law right of access “is rooted in many of the same principles that form the basis of the First Amendment right, including the need for accountability of the otherwise independent judiciary, the need of the public to have confidence in the effective administration of justice, and the need for civic debate and behavior to be informed.” *United States v. Sonin*, -- F. Supp. 3d --, No. 15 Cr. 116, 2016 WL 908650, at \*2 (E.D. Wis. 2016). It attaches to *all* judicial records, and establishes a presumption of access that can be overcome only “if countervailing interests heavily outweigh the public interests in access.” *Rushford v. New Yorker Magazine, Inc.*, 846 F.2d 249, 253 (4th Cir. 1988).

“Regardless of whether the right of access arises from the First Amendment or the common law, it may be abrogated only in unusual circumstances.” *Wash. Post*, 386 F.3d at 576 (quotation marks omitted). The sealing of an entire docket sheet—the openness of which is a prerequisite to accessing any of the underlying docket entries, *Hartford Courant Co. v. Pellegrino*, 380 F.3d 83, 93 (2d Cir. 2004)—is “particularly troubling,” and therefore viewed with special skepticism, *Stone v. Univ. of Md. Med. Sys. Corp.*, 855 F.2d 178, 182 (4th Cir. 1988). Accordingly, the Fourth Circuit has already recognized a right of access to criminal docket sheets,<sup>6</sup> *In re State-Record Co.*, 917 F.2d 129, 129 (4th Cir. 1990) (per curiam), bringing the docket-sheet unsealing sought here squarely within Circuit precedent, *see, e.g., In re Search Warrant for Secretarial Area Outside Office of Gunn*, 855 F.2d 569, 573 (8th Cir. 1988) (“[A] search warrant is certainly an integral part of a criminal prosecution.”).

---

<sup>6</sup> And civil docket sheets. *See Doe v. Pub. Citizen*, 749 F.3d 246, 268–69 (4th Cir. 2014).



As explained more fully below, there is no basis for keeping the docket sheet associated with the malware warrant issued by this Court on July 22, 2013 sealed, and the ACLU's motion should therefore be granted.

**I. The First Amendment requires unsealing the docket sheet listing the malware warrant issued in this District.**

**A. A constitutional right of access applies to the docket sheet listing the malware search warrant.**

To determine whether the First Amendment right of access attaches, a district court must ask first, “whether the place and process have historically been open to the press and general public,” and second, “whether public access plays a significant positive role in the functioning of the particular process in question.” *Press–Enterprise II*, 478 U.S. at 8–10; see *Balt. Sun Co. v. Goetz*, 886 F.2d 60, 64 (4th Cir. 1989).

**1. There is a “centuries-long” tradition of access to docket sheets.**

The “experience” prong of the test is easily satisfied. This country has a “centuries-long history of public access to dockets.” *United States v. Mendoza*, 698 F.3d 1303, 1304 (10th Cir. 2012). “Since the first years of the Republic, state statutes have mandated that clerks maintain records of judicial proceedings in the form of docket books, which were presumed open either by common law or in accordance with particular legislation.” *Pellegrino*, 380 F.3d at 94. Courts, too, have repeatedly affirmed the public’s right to access dockets for a variety of proceedings, civil and criminal. See *Doe v. Pub. Citizen*, 749 F.3d 246, 268–69 (4th Cir. 2014) (civil); *United States v. Ochoa-Vasquez*, 428 F.3d 1015, 1029–30 (11th Cir. 2005) (criminal); *Pellegrino*, 380 F.3d at 96 (civil); *United States v. Valenti*, 987 F.2d 708, 715 (11th Cir. 1993) (criminal); *In re State-Record Co.*, 917 F.2d at 129 (criminal); *Webster Groves Sch. Dist. v. Pulitzer Publ’g Co.*, 898 F.2d 1371, 1377 (8th Cir. 1990) (civil); *Bernstein v. Bernstein*, No. 14 Civ. 6867, 2016 WL

1071107, at \*1 (S.D.N.Y. Mar. 18, 2016) (civil); *In re Application to Unseal 98 Cr. 1101 (ILG)*, 891 F. Supp. 2d 296, 298 (E.D.N.Y. 2012) (criminal); *cf. United States v. Index Newspapers, LLC*, 766 F.3d 1072, 1085 (9th Cir. 2014) (contempt).

To be sure, “the process of issuing search warrants has traditionally not been conducted in an open fashion.” *Gunn*, 855 F.2d at 573; *see Goetz*, 886 F.2d at 64. But even “search warrant applications and receipts are routinely filed with the clerk of court without seal.” *Gunn*, 855 F.2d at 573. And, of course, the historical accessibility of these docket *entries* has depended on the docket *sheets* themselves being publicly accessible. *See id.* at 575 (recognizing First Amendment right to access search warrant docket sheet under history and logic test); *cf. Globe Newspaper Co. v. Fenton*, 819 F. Supp. 89 (D. Mass. 1993) (same as to index of criminal cases). Thus, even when finding sufficient ground to seal a warrant itself, the Fourth Circuit has emphasized that search warrant docket sheets and as many filings on them as possible should nevertheless remain publicly available. *Goetz*, 886 F.2d at 65.<sup>7</sup>

## **2. Logic demands keeping docket sheets open.**

“Logic supports this judgment of history.” *Pellegrino*, 380 F.3d at 95. Docket sheets are not merely judicial records—they “provide a kind of index to judicial proceedings and documents,” without which “the ability of the public and press to attend civil and criminal cases would be merely theoretical.” *Id.* at 93. By the same token, the ability of the public to exercise its

---

<sup>7</sup> The ACLU is aware of only one occasion on which a right of access to a search-warrant docket sheet was found to be lacking. *See In re Search of Fair Fin.*, 692 F.3d 424 (6th Cir. 2012). The Sixth Circuit found no right of access to “documents filed in search warrant proceedings,” and summarily extended this conclusion to the docket sheet itself. *Id.* at 433. The court assumed that docket sheets could be sealed because “docket entries are often detailed and could reveal . . . sensitive information,” without assessing history or logic, *id.*, both of which, as explained here, favor openness. It also ignored the tailoring requirement, which favors redactions over wholesale sealing as the proper approach to sensitive information. *See infra* Part I.B.

right to access any individual entries on a docket sheet is foreclosed when the entire docket sheet is sealed. *See Pub. Citizen*, 749 F.3d at 268 (“Our skepticism toward wholesale sealing of docket sheets [i]s grounded in the commonsensical observation that most of the information contained on a docket sheet is material that is presumptively open to public inspection.”); *Pellegrino*, 380 F.3d at 94 (“Sealed docket sheets would also frustrate the ability of the press and the public to inspect those documents, such as transcripts, that we have held presumptively open.”). Sealing docket sheets also “thwart[s] appellate or collateral review of the underlying sealing decisions. Without open docket sheets, a reviewing court cannot ascertain whether judicial sealing orders exist.” *Id.* This is a particularly salient problem in the Fourth Circuit, where procedures governing judicial sealing orders are constitutionally compelled: a district court must provide notice to the public of the request to seal and an opportunity for the public to challenge the request; consider less-drastring alternatives to sealing; and state any reasons for sealing, supported by specific factual findings, on the record. *Stone*, 855 F.2d at 181; *see also United States v. Mohamed*, No. 13 Cr. 120, 2015 WL 224408, at \*2 (E.D. Va. Jan. 14, 2015) (observing that these procedures are compelled by due process). When the docket sheet itself is sealed, there is no way to enforce these procedural rights.

The significance of the right of access is, moreover, at its “apex” where, as here, the underlying action implicates “not only functions of the courts but also the positions that its elected officials and government agencies take in litigation.” *Pub. Citizen*, 749 F.3d at 271. “[I]n such circumstances, the public’s right to know what the executive branch is about coalesces with the concomitant right of the citizenry to appraise the judicial branch.” *FTC v. Standard Fin. Mgmt. Corp.*, 830 F.2d 404, 410 (1st Cir. 1987). This case involves judicial approval of the executive branch’s use of novel technologies that stretch the limits of existing law. It is crucial

for the public to be able to engage in an informed debate about such phenomena. The sealing of the docket sheet containing the malware warrant makes this impossible. Unsealing would, at the very least, confirm the existence of the warrant in question and the circumstances of its having been authorized and sealed. These would be crucial steps in informing an urgent public debate.

\* \* \*

For these reasons, public access to docket sheets in general—and the search warrant docket sheet at issue in this case in particular—is necessary for the proper “functioning of the judicial process and the government as a whole.” *Globe Newspaper*, 457 U.S. at 606.

**B. There is no governmental interest that outweighs the public’s right of access to the malware-warrant docket sheet, and even if there were, sealing the docket sheet is not a tailored means of accommodating that interest.**

Once the First Amendment right of access attaches, the burden to overcome it “rests on the party seeking to restrict access, and that party must present specific reasons in support of its position.” *Wash. Post*, 386 F.3d at 575. Access may only be denied if the party can demonstrate a “compelling governmental interest” in support of closure and prove that closure is “narrowly tailored to serve that interest.” *Globe*, 457 U.S. at 606–07.

There is, to be sure, a legitimate governmental interest in protecting the integrity of an ongoing investigation. As the Fourth Circuit has recognized, however, “it is not enough simply to assert this general principle without providing specific underlying reasons for the district court to understand how the integrity of the investigation reasonably could be affected by the release of [the] information [sought].” *Wash. Post*, 386 F.3d at 579. “Whether this general interest is applicable in a given case will depend on the specific facts and circumstances presented in support of the effort to restrict public access.” *Id.*

The malware warrant in question here was issued by this Court in mid-2013, and by the end of 2014 the sole prosecution known to the ACLU to have resulted from it had already been resolved. *See* Klein Press Release. The existence of the malware operation, moreover, has been officially acknowledged by the FBI. 2013 Pouslen Article. Thus, “the genie is out of the bottle” with respect to information the government may have once had a legitimate interest in protecting. *In re Application to Unseal 98 CR. 1101 (JLG)*, 891 F. Supp. 2d 296, 300 (E.D.N.Y. 2012). What remains secret, however, is the very “index” to the proceedings that authorized the deployment of malware. *Pellegrino*, 380 F.3d at 91. Perversely, then, the public is aware of the investigation’s existence, and experts have even been able to analyze the malware used by the government, but the most basic details regarding the circumstances under which this operation was judicially authorized remain hidden. The public has a vital interest in knowing this information, which would greatly contribute to the ongoing public debate about the use of malware by law enforcement, and the government has no legitimate interest in keeping it secret.

There is, moreover, an obvious narrower alternative to the wholesale sealing of a docket sheet: the sealing of individual docket entries or, more likely, the redaction of sensitive information from those entries. “[C]areful redaction is clearly a less restrictive means of advancing the state interest.” *United States v. Martin*, 684 F. Supp. 341, 343 (D. Mass. 1988) (alteration omitted). As the Fourth Circuit has recognized, “it would be an unusual case in which alternatives [to wholesale sealing] could not be used to preserve public access to at least a portion of the record.” *Stone*, 855 F.2d at 182. Accordingly, requests to seal entire docket sheets are routinely rejected as overbroad. *See In re State-Record Co.*, 917 F.2d at 129; *Gunn*, 855 F.2d at 575. That same result should obtain here.

There is, then, no sufficient government interest in keeping the docket sheet itself secret; indeed, until the docket sheet is unsealed, it cannot even be determined whether any individual docket entries should remain sealed. Sealing the docket sheet is an overbroad approach to addressing an undemonstrated interest, and it therefore violates the public's First Amendment right of access.

**II. The common law also requires unsealing the malware docket sheet.**

The common-law right of access attaches to “*all* ‘judicial records and documents’”—thus obviating the need to apply the “history and logic” test—and can only be “rebutted if countervailing interests heavily outweigh the public interests in access.” *Wash. Post*, 386 F.3d at 575 (emphasis added). The common-law presumption of access is particularly strong when the entire record of a case is sealed. *See Oliner v. Kontrabecki*, 745 F.3d 1024, 1025–26 (9th Cir. 2014); *Perez-Guerrero v. U.S. Atty. Gen.*, 717 F.3d 1224, 1235 (11th Cir. 2013). Factors to assess in determining whether the common-law presumption has been overcome include “whether the records are sought for improper purposes, such as promoting public scandals or unfairly gaining a business advantage; whether release would enhance the public’s understanding of an important historical event; and whether the public has already had access to the information contained in the records.” *Wash. Post*, 386 F.3d at 575.

For reasons similar to those explained above, the sealing of the search warrant docket sheet also violated the public’s common-law right of access. Much of the information protected by the seal—such as the existence of the malware operation, its timing, and the websites targeted—“has already become a matter of public knowledge,” which obviates the justification for keeping it secret. *Id.* at 579. At the same time, there is important information on the docket sheet about the judicial authorization of the investigation that would “enhance the public’s

understanding of an important historical event,” *id.* at 575, such as the existence of any judicial reasoning behind the approval and any justifications offered by the government for the wholesale sealing. (The absence of this information on the docket sheet would be equally valuable to know.) Indeed, the mere fact of judicial approval has never been confirmed. The government could hardly claim an interest in preserving the secrecy of this fact. The public, on the other hand, has a strong interest in confirming that there was judicial approval of this extraordinary investigative technique—something it cannot do without access to the docket sheet in question.

It is, in short, difficult to “understand how the docket entry sheet could be prejudicial” in any way to the government’s interests, but easy, on the other hand, to see how disclosure would benefit the public. *In re State-Record Co.*, 917 F.2d at 129. Like the First Amendment, the common law therefore requires unsealing.

### Conclusion

For the reasons explained above, the ACLU respectfully requests that this Court unseal any sealed docket sheets associated with any malware warrants issued by this Court on July 22, 2013.

August 25, 2016

Respectfully submitted,

Brett Max Kaufman (*pro hac vice* to be filed)  
Nathan Freed Wessler (*pro hac vice* to be filed)  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION  
125 Broad St., 18th Floor  
New York, NY 10004  
Tel: (212) 549-2500  
Fax: (212) 549-2654  
Email: bkaufman@aclu.org



---

David Rocah (Bar No. 27315)  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION OF MARYLAND  
3600 Clipper Mill Road  
Suite 350  
Baltimore, MD 21211  
Tel: (410) 889-8550  
Fax: (410) 366-7838  
Email: rocah@aclu-md.org

**Certificate of Service**

Information regarding the Assistant United States Attorney responsible for the potentially sealed docket sheets is unavailable. However, I hereby certify that on August 25, 2016, I filed the foregoing motion and memorandum of law with the Clerk of the Court and served the same upon the following individual via First Class U.S. Mail:

Rod J. Rosenstein  
United States Attorney for the  
District of Maryland  
36 S. Charles Street, 4th Floor  
Baltimore, MD 21201

August 25, 2016



---

David Rocah (Bar No. 27315)



**Exhibit A:**

Public Docket Sheet for  
*United States v. Klein*, 13 Mj. 00117 (D. Vt.)

**U.S. District Court  
District of Vermont (Burlington)  
CRIMINAL DOCKET FOR CASE #: 2:13-mj-00117-jmc-1**

Case title: USA v. Klein

Date Filed: 11/20/2013

Date Terminated: 11/22/2013

Assigned to: Judge John M. Conroy

**Defendant (1)****Grant L. Klein***TERMINATED: 11/22/2013*represented by **FPD**

Office of the Federal Public Defender  
District of Vermont  
126 College Street, Suite 410  
Burlington, VT 05401  
(802) 862-6990

Email: samantha\_barrett@fd.org

*TERMINATED: 01/09/2014***ATTORNEY TO BE NOTICED***Designation: Public Defender or  
Community Defender Appointment***David L. McColgin , AFD**

Office of the Federal Public Defender  
District of Vermont  
126 College Street, Suite 410  
Burlington, VT 05401  
(802) 862-6990

Fax: (802) 862-7836

Email: David\_McColgin@fd.org

**ATTORNEY TO BE NOTICED***Designation: Public Defender or  
Community Defender Appointment***Pending Counts**

18:2251A(a)(2) and (b)(1); 18:2252(A)(a)  
(5)(B).F ACTIVITIES RE MATERIAL  
CONSTITUTING/CONT CHILD  
PORNOGRAPHY - receipt/attempted  
receipt of child pornography; access with  
intent to view child pornography  
(1)

**Disposition****Highest Offense Level (Opening)**

Felony

**Terminated Counts****Disposition**

None

**Highest Offense Level (Terminated)**

None

**Complaints****Disposition**

None

**Plaintiff**

USA

represented by **Barbara A. Masterson , AUSA**  
 United States Attorney's Office  
 District of Vermont  
 P.O. Box 570  
 Burlington, VT 05402-0570  
 (802) 951-6725  
 Email: barbara.masterson@usdoj.gov  
**ATTORNEY TO BE NOTICED**

<b>Date Filed</b>	<b>#</b>	<b>Docket Text</b>
11/20/2013	<a href="#">1</a>	APPLICATION for Search Warrant as to In Re: 71 Western Avenue, Brattleboro, Vermont 05301-6914. (Attachments: # <a href="#">1</a> Attachment A, # <a href="#">2</a> Attachment B, # <a href="#">3</a> Affidavit of Jeffrey W. Alford) (hbc) Unsealed on 7/10/2014 pursuant to Order (Document No. 23) in 2:14-cr-66 (law). (Entered: 11/20/2013)
11/20/2013	<a href="#">3</a>	MOTION to Seal Documents by USA re: <a href="#">1</a> Application and Search Warrant as to In Re: 71 Western Avenue, Brattleboro, Vermont 05301-6914. (hbc) Modified on 7/10/2014 pursuant to Order (Document No. 23) in 2:14-cr-66 (law). (Entered: 11/20/2013)
11/20/2013	<a href="#">4</a>	ORDER granting <a href="#">3</a> MOTION to Seal Documents re: <a href="#">1</a> Application and Search Warrant as to In Re: 71 Western Avenue, Brattleboro, Vermont 05301-6914. Signed by Judge John M. Conroy on 11/20/2013. (hbc) Modified on 7/10/2014 pursuant to Order (Document No. 23) in 2:14-cr-66 (law). (Entered: 11/20/2013)
11/22/2013	<a href="#">5</a>	RULE 5(c)(3) Documents Received from District of Maryland as to Grant L. Klein. (Attachments: # <a href="#">1</a> Motion to Seal Criminal Complaint, # <a href="#">2</a> Arrest Warrant (image is sealed))(law) (Entered: 11/22/2013)
11/22/2013	<a href="#">6</a>	MOTION for Detention by USA as to Grant L. Klein. (Attachments: # <a href="#">1</a> Exhibit 1, # <a href="#">2</a> Certificate of Service)(law) (Entered: 11/22/2013)
11/22/2013	<a href="#">7</a>	ORDER Appointing FPD for Grant L. Klein. Signed by Deputy Clerk on 11/22/2013. (hbc) (Entered: 11/22/2013)
11/22/2013	8	MINUTE ENTRY for proceedings held before Judge John M. Conroy. Initial Appearance in Rule 5(c)(3) Proceedings as to Grant L. Klein held on 11/22/2013. Deft present with David McColgin, AFD and Barbara Masterson, AUSA present for gov't. Court informs deft of rights. Deft sworn and Court makes inquiries. Deft waives identity hearing but requests preliminary hearing be held in prosecuting district. Gov't moves for detention. Statements by counsel. ORDERED: Court appoints FPD on behalf of deft. <a href="#">6</a> MOTION for

		Detention is granted. Deft to be detained pending removal to the District of Maryland. (Court Reporter: Recorded) (hbc) (Entered: 11/22/2013)
11/22/2013	<a href="#">9</a>	CJA 23 Financial Affidavit as to Grant L. Klein. (Document image is sealed). (hbc) (Entered: 11/22/2013)
11/22/2013	<a href="#">10</a>	WAIVER of Rule 5(c)(3) Hearing by Grant L. Klein. (hbc) (Entered: 11/22/2013)
11/22/2013	<a href="#">11</a>	COMMITMENT TO ANOTHER DISTRICT as to Grant L. Klein. Defendant committed to District of Maryland (Greenbelt). Signed by Judge John M. Conroy on 11/22/2013. (hbc) (Entered: 11/22/2013)
01/09/2014	<a href="#">13</a>	NOTICE OF APPEARANCE by David L. McColgin, AFPD appearing for Grant L. Klein .(McColgin, David) (Entered: 01/09/2014)

<b>PACER Service Center</b>			
<b>Transaction Receipt</b>			
07/05/2016 13:04:17			
<b>PACER Login:</b>	bgoodaclu	<b>Client Code:</b>	
<b>Description:</b>	Docket Report	<b>Search Criteria:</b>	2:13-mj-00117-jmc
<b>Billable Pages:</b>	2	<b>Cost:</b>	0.20

**Exhibit B:**

Warrant Application in  
*United States v. Klein*, 13 Mj. 00117 (D. Vt.)

UNITED STATES DISTRICT COURT

U.S. DISTRICT COURT  
DISTRICT OF VERMONT  
FILED

for the  
District of Vermont

2013 NOV 20 PM 2:57

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

71 Western Avenue, Apartment 101  
Brattleboro, Vermont 05301-6914

CLERK  
BY HJC  
DEPUTY CLERK

Case No. 2:13-mj-117

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

located in the \_\_\_\_\_ District of \_\_\_\_\_ Vermont \_\_\_\_\_, 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:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 2252, 2252A	Possession, access with intent to view, distribution and receipt of Child Pornography

The application is based on these facts:

See Attached Affidavit.

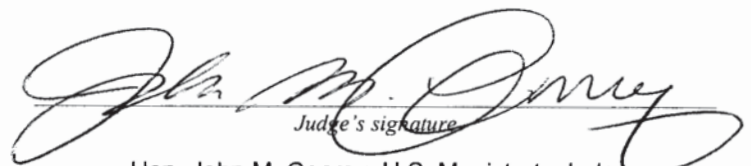
- Continued on the attached sheet.
- Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature  
 Jeffrey Alford, FBI Special Agent  
 Printed name and title

Sworn to before me and signed in my presence.

Date: 11/20/2013

City and state: Burlington, Vermont

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

**Exhibit C:**

Affidavit of Special Agent Jeffrey W. Alford in Support  
of Search Warrant Application in  
*United States v. Klein*, 13 Mj. 00117 (D. Vt.)

**AFFIDAVIT**

I, Jeffrey W. Alford, being first duly sworn, hereby depose and state as follows:

**Introduction**

1. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation, currently assigned to the Albany, New York Division in the Rutland, Vermont Office. I have been an FBI Special Agent for 22 years. As a Special Agent, I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), authorized to investigate violations of Federal law and to execute warrants issued under the authority of the United States. I am currently responsible for conducting investigations in a variety of criminal matters, to include computer-related crimes. I am empowered to conduct investigations of, and to make arrests for, felony offenses to include those involving the sexual exploitation of children, as enumerated in Title 18, United States Code, Chapter 110, and in particular Sections 2252 and 2252A, which criminalize the receipt, distribution, or possession of, or the knowing access with intent to view, child pornography.

2. As a Special Agent, I have participated in the execution of numerous search warrants, to include those resulting in seizure of computers and electronic storage media with regard to violations of Federal law. In my experience, I have observed numerous examples of child pornography stored on computer media and have received training relative to investigating child pornography. I know 18 U.S.C §§ 2252(a)(2), 2252(b)(1), 2252A(a)(2)(A), and 2252A(b)(1), make it a crime to knowingly receive or distribute, or attempt or conspire to knowingly receive or distribute, child pornography transported in interstate or foreign commerce, including by computer; and 18 U.S.C. §§ 2252(a)(4), 2252(b)(2), 2252A(a)(5)(B), and 2252A(b)(2) make it a Federal offense for any person to knowingly possess, access with intent to



view, or attempt or conspire to access with intent to view, child pornography transported in interstate or foreign commerce, including by computer.

**Background**

3. This Affidavit is submitted in support of an Application for a search and seizure Warrant for the residence located at: **71 Western Avenue, Apartment 101, Brattleboro, Windham County, Vermont 05301** (hereafter referred to as the "Subject Premises"), to include any computer(s) and computer media located therein, where contraband, evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2), 2252(b)(1), 2252A(a)(2)(A), 2252A(b)(1), 2252(a)(4), 2252(b)(2), 2252A(a)(5)(B), and 2252A(b)(2), as specified further in Attachment B, might be found.

4. I believe that a computer has been used in connection with violations of Title 18, U.S.C. §§ 2252(a)(2), 2252(b)(1), 2252A(a)(2)(A), 2252A(b)(1), 2252(a)(4), 2252(b)(2), 2252A(a)(5)(B), and 2252A(b)(2), with regard to the illegal receipt, distribution, possession, or accessing of child pornography. I believe the items delineated in Attachment B to be contraband, evidence, fruits, instrumentalities of these offenses, and/or property utilized in the commission of these offenses. I respectfully request authority to seize such material from such premises, specifically any computer(s), and related peripherals and media, which could constitute both an instrumentality of the crime and/or a container in which contraband and other evidence of the commission of the crime(s) is or could be enclosed. I request authority to search the entire premises, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

5. I base this Affidavit upon my own experience and background as a Special Agent

of the FBI, as well as investigative information provided and conveyed to me by the FBI's Major Case Coordination Unit in the state of Maryland, which is part of the Violent Crimes Against Children Section under the direction of the Criminal Investigative Division at FBI Headquarters in Washington, D.C. This includes information provided by other FBI Special Agents; written reports about this and other investigations that I have received and reviewed, either directly or indirectly from other law enforcement agents, including those from foreign law enforcement agencies; information gathered from the service of administrative subpoenas; results of physical and electronic surveillance; and independent investigation and analysis by FBI Agents/Analysts and computer forensic professionals.

6. This affidavit is offered for the limited purpose of establishing probable cause and does not include each and every fact in connection with this investigation. I have set forth only those facts that I believe are necessary to establish probable cause that evidence of violations of 18 U.S.C. §§ 2252(a)(2), 2252(b)(1), 2252A(a)(2)(A), 2252A(b)(1), 2252(a)(4), 2252(b)(2), 2252A(a)(5)(B), and 2252A(b)(2) is located at the Subject Premises. Where statements of others are set forth in this Affidavit, they are set forth in substance and in part.

7. To summarize, the following information sets forth facts indicating a computer user at the Subject Premises has accessed, via the Internet, images depicting minors engaging in sexually explicit activity, and contraband, evidence, fruits, instrumentalities of the aforementioned offenses, and/or property used in the commission of such offenses, is located at said premises. The instant investigation, as described below, involves an Internet-based website hereafter referred to as "Website 20."<sup>1</sup> The investigation revealed that an individual who is

---

<sup>1</sup> The particular website described in this affidavit has been referred to in other related legal process by the number used in this affidavit, so this number is being used here for consistency. The actual name of the website is

believed to reside at the Subject Premises voluntarily and intentionally accessed a section of “Website 20” that contained child pornography. The primary purpose of “Website 20” is to advertise and distribute child pornography. I believe that a user of the Internet at such premises knowingly received, possessed, or accessed with intent to view, or attempted to receive, possess, or access with intent to view, child pornography on “Website 20.”

**Definitions of technical terms**

8. The following definitions apply to this affidavit:
- 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” refers to a linked series of posts and reply messages. Message threads 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 user who sent/received such a message, or by the bulletin board administrator.
  - b. “Child erotica,” as used herein, means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.
  - c. “Child Pornography,” as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction 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

---

known to law enforcement and to me. Investigation into the users of this site remains ongoing and disclosure of the name of the site would potentially alert users to the fact that law enforcement action is being taken against the site, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

- d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "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."
- e. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A DNS (domain name system) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as "www.cnn.com", into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.
- f. "Computer hardware," as used herein, consists of all equipment which 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, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, 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, but not limited to, physical keys and locks).
- g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- i. "Computer passwords, pass-phrases 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 or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code 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 progress to restore it.

- j. “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.
- 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. “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, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.
- m. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other

computers.

- n. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- p. "Sexually explicit conduct" 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 genitals or pubic area of any person. See 18 U.S.C. § 2256(2).
- q. "Visual depictions" include 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).
- r. "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).

#### **The Internet and E-Mail**

- 9. Based on my experience, as well as consulting with other special agents, I know the following:
  - a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The

world wide web (“www”) is a functionality of the Internet which allows users of the Internet to share information;

- b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and
- c. E-mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user’s computer, transmitted to the subscriber’s mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

### Computers and Child Pornography

10. Based on my experience, as well as consulting with other Special Agents, I know the following:

- a. Computers and digital technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.
- b. The development of computers and digital cameras has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
- c. Individuals who access with intent to view, possess, distribute, and/or receive child pornography can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with

digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store over 100 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

- d. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
- e. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte (1000 gigabytes) external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them.)
- f. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- g. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services 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 account from any computer 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 or external media in most cases.

- 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 e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may 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 are interested in child pornography**

11. Based on my prior investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have consulted, I believe there are certain characteristics common to individuals who utilize web based bulletin boards to possess, access with intent to view, distribute, and/or receive images of child pornography, specifically:

- a. Individuals who possess, access with intent to view, distribute, and/or receive images of child pornography 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. Individuals who possess, access with intent to view, distribute, and/or receive child pornography 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. Individuals who possess, access with intent to view, distribute, and/or receive child pornography almost always possess and maintain their “hard copies” of child pornographic 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. Individuals who have a sexual interest in children or in images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, individuals who possess, access with intent to view, distribute, and/or receive child pornography 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, to enable the individual to view the child pornography images, which are valued highly.
- e. Individuals who possess, access with intent to view, distribute, and/or receive child pornography 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 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.
- f. Individuals who would have knowledge about how to access a hidden and embedded bulletin board would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a child pornography image.
- g. Individuals who possess, access with intent to view, distribute, and/or receive child pornography 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.

12. Based on the fact that the user of IP Address 50.133.199.243 accessed “Website 20” which contained child pornography and which has as its primary purpose the advertisement and distribution of child pornography, I believe that such computer user likely displays

characteristics common to individuals who possess, access with intent to view, distribute, and/or receive child pornography.

**Searches of computers and related equipment, and seizure of computer systems**

13. Based on my training and experience, and on my communications with other law enforcement personnel, I know the following:

- a. Searches and seizures of evidence from computers commonly requires agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:
  - i. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
  - ii. Searching computer systems for criminal evidence is a highly technical process requiring expert skill 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, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.
- b. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient

search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

- c. Furthermore, because the investigation renders belief that the computer and its storage devices are all instrumentalities of crime(s), within the meaning of 18 U.S.C. § 2251 through 2256, they should all be seized as such.

**Search methodology to be employed**

14. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;
- b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;
- c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- e. surveying various file directories and the individual files they contain;
- f. opening files in order to determine their contents;

- g. scanning storage areas;
- h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and
- i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

#### **Investigation of "Website 20"**

15. Based on my training and experience, and on my communications with other law enforcement personnel involved in this investigation who have direct knowledge of the following, I know the following about "Website 20":

a. "Website 20" is of a format commonly known as an image board, which allows users to upload images to, and download images from, the website. The primary purpose of the website is the advertisement and distribution of child pornography. According to statistics posted on the site, the site contained 3,317 registered members, 5,354 images that were uploaded, and 40 galleries uploaded with 2,362 images as of June 25, 2013.

b. The initial web page contained eight hyperlinks at the top of the web page and numerous data-entry fields in the middle of the web page, including an area to upload files. Located at the bottom of the web page were four additional hyperlinks.

c. A review of the hyperlinks at the bottom of the web page revealed that three of the four contained approximately 174 pages of uploaded images, with approximately 30 images per page. A review of selected pages revealed images that appeared to depict child pornography (CP) and child erotica of prepubescent and early pubescent females. The fourth hyperlink contained one page with approximately 30 images on the page that also appeared to depict CP and child erotica of prepubescent and early pubescent females. Each of the above

images appeared to contain the date and time of uploading, as well as the total number of views. For example, a user posted an image depicting a prepubescent female being orally penetrated by what appeared to be an adult male's penis. This image had been viewed approximately 2,575 times as of June 25, 2013. A user posted an image depicting a naked prepubescent female who was sitting with her legs spread apart, exposing her vagina. Her right hand was pressed against her vagina. This image had been viewed approximately 106 times as of June 25, 2013.

d. No chat features were located on the web page, and no registration was required.

**Court-authorized use of Network Investigative Technique**

16. Based on my training and experience, and on my communications with other law enforcement personnel involved in this investigation who have direct knowledge of the following, I know the following:

a. Websites generally have Internet Protocol (IP) address logs that can be used to locate and identify the site's users. In such cases, after the seizure of a website whose users are engaging in unlawful activity, law enforcement can review those logs in order to determine the IP addresses used to access the site. A publicly available lookup could then be performed to determine what Internet Service Provider ("ISP") owned the target IP address. A subpoena would then be sent to that ISP to determine the user to which the IP address was assigned at a given date and time.

b. IP address logs of "Website 20" users were contained within data examined by law enforcement when data from the computer server hosting "Website 20" was obtained. However, because of the network software utilized by "Website 20," the logs of user activity contained only the IP addresses of the last computer through which the communications

of “Website 20” users were routed before the communications reached their destinations (the destination being “Website 20”). It is not possible to trace such Internet use back through the network to the actual users who sent the communications or requests for information. Those IP address logs therefore could not be used to locate and identify users of “Website 20”; rather, they could only identify the last computer through which users were routed before arriving at “Website 20.”

c. Accordingly, on July 22, 2013, the United States District Court for the District of Maryland authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique (“NIT”) on “Website 20” in an attempt to identify the actual IP addresses and other identifying information of computers used to access “Website 20.” Pursuant to that authorization, between July 31, 2013, and approximately August 5, 2013, each time a user logged into “Website 20” by entering a username and password and/or accessed a section of “Website 20” where child pornography may be accessed, the NIT sent one or more communications directly to the user’s computer. Those communications caused the receiving computer to deliver data to a computer either known to or controlled by the Government, that would help to identify the computer, its location, other information about the computer, and the user of the computer accessing “Website 20.” That data included the computer’s actual IP address and the date and time that the NIT determined what that IP address was, a unique session identifier to distinguish the data from that of other computers, the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86), the computer’s host name, and the computer’s Media Access Control (MAC) address.

**User of IP Address 50.133.199.243 on "Website 20"**

17. Based on my communications with other law enforcement personnel involved in this investigation who have direct knowledge of the following, I know the following:

a. According to data obtained from logs on "Website 20," monitoring by law enforcement, and the deployment of an NIT, on August 04, 2013, from approximately 4:06am until 4:08am UTC, an unknown user utilized Internet Protocol (IP) address 50.133.199.243 to access "Website 20."

b. During this time period, the individual accessed approximately six (6) web pages that contained 171 images. Of the 171 images viewed during this time period, approximately 65 of these images related to child exploitation material or similar content. The images included the following:

i. 5762\_hrjustin001.jpg – image depicts a clothed pre-school age child of indeterminate sex standing between the legs of a partially clothed adult male who is naked from the waist down. The adult male appears to be sitting in a chair near a desk or computer. The adult male's left hand is visibly touching his erect penis and placing it against the minor's mouth.

ii. 5763\_001M013Copy.jpg – image depicts a partially clothed infant male, with a pacifier lying on his chest, naked from the waist down laying on his back with his genitals exposed to the camera. A partially clothed adult male, naked from the waist down, is also visible in the picture. The adult male's erect penis is visibly penetrating the anus of the minor.

iii. 5765\_2112.jpg – image depicts an infant of indeterminate sex apparently asleep. An adult male penis has been placed into the infant's open mouth.



iv. 5772\_2chub15.jpg – image depicts a naked pre-pubescent female and another naked pre-pubescent child of indeterminate gender. The minor female is laying on her back on a bed with her feet toward the camera and her body and legs positioned in such a way that her genitals are exposed to the camera. Additionally, what appears to be handcuffs or shackles are clearly visible on both ankles and the right wrist. Her left arm/wrist is obscured by the second child in the picture.

c. In addition to the previously described site, the individual utilizing IP address 50.133.199.243 was also observed to access another website associated with child exploitation materials, though it did not appear that the user accessed such materials on that second site. Access to this second site occurred on August 4, 2013 between 3:58am and 4:04am UTC.

d. A check conducted of publically available databases showed that IP address 50.133.199.243 is assigned to Internet Service Provider (ISP) Comcast Communications.

e. On August 4, 2013, a subpoena was served upon Comcast Communications for information related to the customer assigned IP address 50.133.199.243 on August 4, 2013 at 3:58am UTC and at 4:06am UTC. On August 6, 2013, Comcast Communications, in response to the issued subpoena, provided the following information related to the customer assigned the captioned IP address during the time period requested:

Name: Susan Klien  
Address: 71 Western Avenue Apartment 101, Brattleboro, VT 05301-6914 (the Subject Premises)

f. Records checks performed at the FBI's Major Case Coordination Unit confirmed that a "Susan Rachel Klein" currently resides at the Subject Premises. Comcast confirmed that the spelling of the last name in their system is "Klien." Records checks showed

Cathy Gray as another potential resident at such address. Checks also showed Susan Klein has an also-known-as name "Susan Gray".

**Investigation of the Subject Premises and Residents**

18. On November 7, 2013, I caused a search to be done of the State of Vermont Department of Motor Vehicles automated records. Based thereon, I learned that the following people reside at the Subject Premises:

- a. Susan R. Klein, nee Susan Gray, female, Operator License Number 12746920. Vermont DMV records also reflect a 2013 Mazda MZ2, license plate GAG603, color black, as a motor vehicle currently registered to Susan Klein at the Subject Premises.
- b. Grant L. Klein, Operator License Number 62741317. Vermont DMV records also reflect a 1999 Ford pickup truck, license plate 170A872, color red, as having been registered to Grant Klein at the Subject Premises. Such registration expired in October 2013.
- c. Cathy M. Gray, Operator License Number 02710749. Vermont DMV records also reflect a 2005 Toyota truck, license plate 189A595, color black; as well as a 2007 Hyundai Accent, license plate FTT804, color blue, as motor vehicles currently registered to Cathy Gray at the Subject Premises.

19. On November 15, 2013, I conducted surveillance of the Subject Premises and observed the following:

- a. I saw a black Toyota Tacoma pickup truck with Vermont registration number 189A595 parked in the driveway to the Subject Premises. This vehicle is registered to Cathy Gray.

b. I also saw a black Mazda vehicle in the driveway, which bore Vermont registration GAG603. This vehicle is registered to Susan Klein. I also saw this vehicle parked in the parking lot of the People's United Bank processing center, located at 629 Putney Road in Brattleboro. On November 18, 2013, I spoke with a security official at the People's United Bank, who confirmed that Susan Klein is employed by People's United Bank at its Operations Center on Putney Road in Brattleboro, Vermont, and that she is listed in the Bank's records as living at the Subject Premises.

20. On November 13, 2013, I spoke with Windham County Department of Corrections Probation and Parole Officer (PO) Henry Farnum, who told me that he supervised Grant Klein from November 9, 2010 until January 10, 2012, following Klein's conviction for Interference with Access to Emergency Services. During his supervision of Klein, PO Farnum visited him at the Subject Premises. PO Farnum recalled Klein's apartment to be accessible on the east side of the building via the driveway which leads to a shed where Klein stored his snowblower. PO Farnum thought Klein's apartment was also accessible from the front door to the building at 71 Western Avenue. PO Farnum recalled that Klein lived at such location with his wife named "Susan" or "Suzanne" and his mother-in-law. On November 14, 2013, I received from PO Farnum a copy of the Brattleboro Probation & Parole Intake Information Form which was completed by Klein upon being placed on probation. This form indicated his residence to be the Subject Premises, a green building on the corner of Speno Court, and that he lived with Susan Klein and Cathy Gray.

21. On November 7, 2013, I caused an open source database query to be conducted which showed that as of November 2012, Susan Klein (or Klien), Grant Klein, and Cathy Gray reside together at the Subject Premises.

22. On November 15, 2013, I received information from the US Postal Inspection Service, Manchester, New Hampshire Office, which indicated that Susan Klein is an authorized mail recipient at the Subject Premises.

23. On November 19, 2013, I received information from Comcast which indicated that as of November 17, 2013, the subscriber to the Subject Premises is Susan Klien. Susan Klien is the same name of the subscriber to the Subject Premises on August 4, 2013.

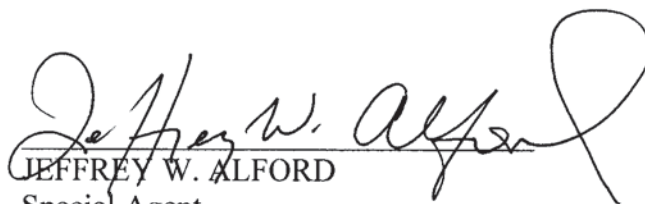
#### **Conclusion**

24. Based on the foregoing factual information, with my training and experience, and information provided and conveyed to me by the FBI's Major Case Coordination Unit and other law enforcement personnel working on this investigation, I believe that violations of Title 18, United States Code, Sections 2252(a)(2), 2252(b)(1), 2252A(a)(2)(A), 2252A(b)(1), 2252(a)(4), 2252(b)(2), 2252A(a)(5)(B), and 2252A(b)(2), have been committed and that contraband, evidence, fruits, instrumentalities of those offenses, and/or property used for committing those offenses, to include a computer, are located at the premises known as 71 Western Avenue, Apartment 101, Brattleboro, Windham County, Vermont 05301 (the Subject Premises), which is more particularly described in Attachment A.

25. I further believe that off-site forensic analysis of the computer(s), and/or computer-related equipment and storage devices and media, seized from the Subject Premises will yield evidence in the form of child pornography contraband, and other electronic evidence

of violations of Title 18, United States Code, Sections 2252(a)(2), 2252(b)(1), 2252A(a)(2)(A), 2252A(b)(1), 2252(a)(4), 2252(b)(2), 2252A(a)(5)(B), and 2252A(b)(2).

26. Based upon the foregoing, I respectfully request this Court to issue a warrant to search the residence located at 71 Western Avenue, Apartment 101, Brattleboro, Windham County, Vermont 05301 (the Subject Premises), which is described more particularly in Attachment A, authorizing the search for, and seizure of, items described in Attachment B, and a subsequent, more thorough, highly technical search of those items in a secure and controlled off-site environment.

  
JEFFREY W. ALFORD  
Special Agent  
Federal Bureau of Investigation

Sworn to and subscribed before me this 20<sup>th</sup> day of November, 2013

  
HON. JOHN M. CONROY  
United States Magistrate Judge