

ORIGINAL
RECEIVED
SUPREME COURT
STATE OF WASHINGTON
2007 FEB 12 P 3:01

No. 793719

IN THE SUPREME COURT
OF THE STATE OF WASHINGTON

CLERK

STATE OF WASHINGTON,

Petitioner/Respondent,

v.

MICHAEL ALLAN BOYD, Petitioner,

LEE GILES, Respondent,

MAUREEN ELIZABETH WEAR, Respondent

CLERK

2007 FEB 20 P 11:41

FILED
SUPREME COURT
STATE OF WASHINGTON

BRIEF *AMICUS CURIAE*
OF
WASHINGTON ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE
LAWYERS

Sheryl Gordon McCloud
WSBA No. 16709
Law Offices of Sheryl Gordon
McCloud
710 Cherry Street
Seattle, WA 98104-1925
(206) 224-8777
Attorney for Amicus NACDL

Colin Fieman 80294
Georgia Bar No. 259690
1331 Broadway, Suite 400
Tacoma, Washington 98402
(253) 593-6710
Attorney for Amicus WACDL

Laura E. Mate
WSBA No. 28637
1601 Fifth Ave., Suite 700
Seattle, WA 98101
(206) 553-1100
Attorney for Amicus WACDL

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	ii
I. INTRODUCTION	1
II. A DEFENDANT’S FUNDAMENTAL RIGHT TO INDEPENDENTLY EXAMINE THE EVIDENCE AGAINST HER	5
III. THE CRITICAL NEED FOR INDEPENDENT FORENSIC ANALYSIS IN COMPUTER CASES	10
IV. REASONABLE AND EFFECTIVE “PROTECTIVE ORDERS” HAVE BEEN USED BY BOTH FEDERAL AND WASHINGTON COURTS.	15
V. CONCLUSION	20

TABLE OF AUTHORITIES

	Page
STATE CASES	
<i>City of Fieldcrest v. Jensen</i> , 158 Wash. 2d 384, 143 P.3d 776 (2006)	3
<i>State v. Boehme</i> , 71 Wash. 2d 621, 430 P.2d 527 (1967)	15
<i>State v. Kilburn</i> , 151 Wash. 2d 36, 84 P.3d 1215 (2004)	5
<i>State v. Pawlyk</i> , 115 Wash. 2d 457, 800 P.2d 338 (1990)	19
<i>State v. Punsalan</i> , 156 Wash. 2d 875, 133 P.3d 934 (2006)	6
<i>Matter of Williams</i> , 121 Wash. 2d 655, 853 P.2d 444 (1993)	5
<i>Williams v. Texas</i> , 958 S.W.2d 186 (Tex. Crim. App. 1997)	8
FEDERAL CASES	
<i>Ake v. Oklahoma</i> , 470 U.S. 68 (1985)	6
<i>Clark v. Martinez</i> , 543 U.S. 371 (2005)	5, 6
<i>Hickman v. Taylor</i> , 329 U.S. 495 (1947)	8
<i>Strickland v. Washington</i> , 466 U.S. 668 (1984)	6
<i>United States v. Abreu</i> , 202 F.3d 386 (1st Cir. 2000)	8
<i>United States v. Frabizio</i> , 341 F. Supp. 2d 47 (D. Mass. 2004)	8
<i>United States v. Hill</i> , 322 F. Supp. 2d 1081 (C.D. Cal. 2004)	7
<i>United States v. Knellinger</i> , ___ F. Supp. 2d ___, 2007 WL 219984 (E.D. Va., Jan. 25, 2007)	<i>passim</i>

	Page
<i>United States v. Lee</i> , CR04-5281 RBL (W.D. Wa. 2005)	<i>passim</i>
<i>United States v. Nobles</i> , 422 U.S. 225 (1975)	9
<i>Wardius v. Oregon</i> , 412 U.S. 470 (1973)	15
<i>Wiggins v. Smith</i> , 539 U.S. 510 (2003)	6

STATE STATUTES

RCW 9.68A.050	<i>passim</i>
---------------------	---------------

FEDERAL STATUTES

18 U.S.C. § 2252	2
18 U.S.C. §3509	<i>passim</i>

OTHER AUTHORITIES

CrR 3.1	7
CrR 4.7	<i>passim</i>
U.S. Const. amend. VI	6
U.S. Const. amend. XIV	6
Wash. Const. art. 1, § 22	6
Orrin Kerr, <i>Searches & Seizures in a Digital World</i> , 119 Harv. L. Rev. 531 (Dec. 2005)	10, 11

Ty E. Howard, *Don't Cache out Your Case: Prosecuting Child
Pornography Possession Law Based on Images Located in Temporary
Internet Files*, 19 Berkeley Tech L.J. 1227 (Fall 2004) 11

I. INTRODUCTION

The cases before the Court involve the scope of discovery to be accorded defendants when the evidence includes alleged “depictions of a minor engaged in sexually explicit conduct.” In *State v. Giles* and *State v. Wear*, the evidence at issue consists of videotapes, printed pictures and magazines. The trial court in *Giles* directed the State to turn over copies of the contraband under the terms of a protective order designed to prevent dissemination of the materials.

In *State v. Boyd*, much of the evidence consists of images that were recovered from the defendant’s computer and other digital storage devices. Because of the forensic issues that typically attend criminal cases involving computers and digital images, there is usually a compelling need for the defense to obtain exact “mirror image” copies of the defendant’s computer hard drive and other storage devices for independent forensic analysis. See Sec. III, *infra*. Nevertheless, the trial court in *Boyd* denied the defense an opportunity meaningfully to examine the computer evidence.

That the trial courts reached different results is surprising in light of CrR 4.7(a)’s provision for mandatory disclosure of the evidence. The

State argues this rule does not obligate it to provide the defense with copies of the evidence containing or depicting child pornography because the rule conflicts with RCW 9.68A.050's prohibition on the duplication and dissemination of such images. State's Statement of Grounds for Direct Review in *Giles* ("State's Statement in *Giles*") at 9. In fact, the State interprets the statute as imposing a blanket prohibition on duplication of alleged child pornography images for the defense. State's Statement in *Giles* at 6. That interpretation cannot be correct because an absolute prohibition on duplication would deprive defendants of their constitutional rights to effective assistance of counsel and to present a defense.

Under the doctrine of constitutional avoidance, this Court construes statutes in a manner consistent with the demands of the Constitution. Given the constitutional implications, a better reading of the statute is that, while it does not specifically address discovery, it also does not preclude duplication of evidence necessary to the effective assistance of counsel. Consistent with this reading, federal courts, faced with similar prohibitions on duplication (*see* 18 U.S.C. § 2252), have nonetheless ordered prosecutors to duplicate and disclose child pornography evidence to defendants.

Moreover, defendants have a procedural right to discovery. If there is a conflict between RCW 9.68A.050 and CrR 4.7, the rule controls. *See City of Fieldcrest v. Jensen*, 158 Wash. 2d 384, 143 P.3d 776, 794 (2006) (“If the right is substantive, the statute prevails; if it is procedural, then the court rule prevails.” (internal quotations omitted)).

The State’s argument also fails to take into account the reference in CrR 4.7(a) to “protective orders,” which appears to allow trial courts to impose reasonable safeguards on the handling of sensitive evidence. The State in other child pornography cases has entered into stipulated protective orders similar to the one entered in *Giles*, and the State has offered no facts that might show why such an order would be inadequate in the instant cases. *See* Apps. C-F, and Sec. IV, *infra*.

The State makes the alternative argument that discovery in these cases is governed by CrR 4.7(e) for “Discretionary Disclosures” rather than 4.7(a). Response to Motion for Discretionary Review in *Boyd* at 7-8. This position is premised on the idea that CrR 4.7(a) only requires “disclosure,” not “duplication.” *Id.* at 8. This interpretation of the rule, however, also fails. The word “disclose” must be interpreted in a manner consistent with the demands of the Constitution. In some cases, to ensure

effective assistance of counsel and to present a defense, the defense must have its own copy of critical evidence. *See* Sec. III, *infra*.

If, however, the Court believes 4.7(e) is the controlling subsection, the discovery defendants seek is still appropriate because they have made adequate showings of materiality and the State has made no showing of “substantial risk.” Moreover, should this Court have any question regarding the sufficiency of the showings, it should remand to allow the parties an opportunity to fully develop the record with a better understanding of the governing standards.

Amici urge this Court to reaffirm that defendants have a fundamental right to thoroughly examine the evidence against them, and that includes the right independently to analyze evidence outside the presence of the prosecution. At the same time, discovery need not be unlimited to allow for an effective defense. There are conditions that trial courts can impose on discovery that will ensure that child pornography is not mishandled, without unduly limiting a defendant’s trial preparations or tilting the discovery process too far in the prosecution’s favor. This brief will suggest ways to balance the discovery process in child pornography

cases that are consistent with constitutional requirements and avoid the essentially all-or-nothing approach advocated by the State.

II. A DEFENDANT’S FUNDAMENTAL RIGHT TO INDEPENDENTLY EXAMINE THE EVIDENCE AGAINST HER

The State argues that RCW 9.68A.050 prohibits it from ever providing defense counsel with a copy of a computer hard drive, video or other media that contain child pornography. State’s Statement of Grounds for Direct Review in *Giles at Wear* at 6-7. The doctrine of constitutional avoidance, however, demands a different interpretation of the statute. The doctrine is “a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts.” *Clark v. Martinez*, 543 U.S. 371, 380 (2005). As this Court has stated: “It is a general rule that statutes are construed to avoid constitutional difficulties when such construction is consistent with the purposes of the statute.” *Matter of Williams*, 121 Wash. 2d 655, 853 P.2d 444 (1993) (construing statute to avoid equal protection problems); *see also State v. Kilburn*, 151 Wash. 2d 36, 43, 84 P.3d 1215 (2004).

To preclude the defense from ever possessing such images in many cases would lead to denial of a defendant's rights to effective assistance of counsel and to present a defense.¹ See U.S. Const. amends. VI and XIV; Wash. Const. art. 1, § 22. In *Strickland v. Washington*, the United States Supreme Court recognized that the right to effective assistance of counsel includes the right to have counsel conduct a "reasonable investigation[]." 466 U.S. 668, 690-91 (1984); see also *Wiggins v. Smith*, 539 U.S. 510, 523, 525 (2003).²

This Court has also recently recognized that "[t]he Sixth Amendment right to effective assistance of counsel includes expert assistance necessary to an adequate defense." *State v. Punsalan*, 156 Wash. 2d 875, 878, 133 P.3d 934 (2006), citing *Ake v. Oklahoma*, 470

¹Under the doctrine of constitutional avoidance, it is not necessary that every application of the statute would violate the constitution. As the United States Supreme Court recently stated: "When deciding which of two plausible statutory constructions to adopt, a court must consider the necessary consequences of its choice. If one of them would raise a multitude of constitutional problems, the other should prevail – *whether or not those constitutional problems pertain to the particular litigant before the court.*" *Clark*, 543 U.S. at 380-81.

²The State concedes this constitutional issue to a point: "a criminal defendant's Sixth Amendment right to counsel entitles him to an attorney who is prepared for trial, and that preparation includes reviewing the physical evidence, including contraband, that may be admitted in the prosecution's case-in-chief." State's Statement in *Giles* at 7. But "reviewing" does not always satisfy the lawyer's duty to investigate, particularly where an adequate investigation requires expert assistance.

U.S. 68, 76, 83 (1985) (due process guarantees the defendant access to competent experts “who will conduct an appropriate examination and assist in evaluation, preparation, and presentation of the defense”). To conduct adequate investigations and obtain expert opinions, attorneys and their experts need not only nominal access to the evidence, but also an opportunity for independent examination. Sometimes this can be satisfied by examining evidence at the police station but, as demonstrated below, in many cases it is practically impossible to do so. *See, e.g., United States v. Knellinger*, ___ F. Supp. 2d ___, 2007 WL 219984, at *6 (E.D. Va., Jan. 25, 2007) (“the practical consequences of all these difficulties is that . . . [the expert] would not agree to work on a case like Knellinger’s because he could not feasibly move his equipment to, or properly do his work in, a Government facility”); *United States v. Hill*, 322 F. Supp. 2d 1081, 1092 (C.D. Cal. 2004) (requiring expert to examine media in government lab is “unreasonably burdensome” and “inadequate”).

Even when not practically impossible, an unbending requirement that defense counsel must examine evidence at the police station may force counsel to choose between revealing defense strategies and expert assistance. Indeed, the provision in CrR 3.1 that a defendant’s motion for

expert services “may be made *ex parte*” is rendered meaningless if the expert must work under the scrutiny of the prosecution and risk exposing work-product.³ The United States Supreme Court has observed “it is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel.” *Hickman v. Taylor*, 329 U.S. 495, 510 (1947). *See also United States v. Abreu*, 202 F.3d 386 (1st Cir. 2000) (federal law provides for *ex parte* proceedings when appointed counsel requests funding for experts “so as to ‘prevent[] the possibility that an open hearing may cause a defendant to reveal his defense’” (citation omitted)); *Williams v. Texas*, 958 S.W.2d 186, 193 (Tex. Crim. App. 1997) (A defendant should not be “forced to choose between either forgoing the appointment of an expert or disclosing to the State in some detail his defensive theories or theories about weaknesses in the State’s case”).

Although the work-product doctrine “most frequently is asserted as a bar to discovery in civil litigation, its role in assuring the proper functioning of the criminal justice system is even more vital. The interests

³*See, e.g., United States v. Frabizio*, 341 F. Supp. 2d 47, 49 (D. Mass. 2004) (noting defendant’s submittal that “any tests conducted on an FBI computer will leave behind a roadmap of the process and its results on that computer’s hard drive”).

of society and the accused in obtaining a fair and accurate resolution of the question of guilt or innocence demand that adequate safeguards assure the thorough preparation and presentation of each side of the case.” *United States v. Nobles*, 422 U.S. 225, 238 (1975). Because defense attorneys must often rely on investigators and other agents, the doctrine extends to their work-product as well. *See id.* at 238-39.

All of these issues can be avoided, however, by reading RCW 9.68A.050 to allow duplication and disclosure, under carefully drafted protective orders, for the limited purpose of discovery in connection with criminal proceedings. *See* Sec. IV, *infra*. That is precisely what a federal district court did when interpreting the recently enacted “Adam Walsh” Act, 18 U.S.C. § 3509, which addresses discovery in child pornography cases. *See Knellinger*, 2007 WL 219984. In *Knellinger*, applying the doctrine of constitutional avoidance, the court concluded the statute “must be read to include at least every opportunity for inspection, viewing, and examination required by the Constitution.” 2007 WL 219984 at *3-*4. In the cases before this Court, however, the State urges the Court to adopt an interpretation of RCW 9.68A.050 that not only would render it far more

restrictive than the Adam Walsh Act but, more importantly, would inevitably result in infringement of defendants' constitutional rights.

III. THE CRITICAL NEED FOR INDEPENDENT FORENSIC ANALYSIS IN COMPUTER CASES

Most child pornography cases now involve images that have been transmitted over the Internet and stored on a computer hard drive or other digital media, such as a CD or "zip drive." And, in most cases involving digital images, a defense attorney will be ineffective if she does not get an independent forensic analysis of the hard drive or other digital media.

As one recent article has noted, "Computers can only store data, but the amount of data is staggering." Orrin Kerr, *Searches & Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (Dec. 2005). This data includes evidence of who has used the computer and when, their Internet activities, whether the computer was infected with "malicious codes" (or "viruses," including ones that allow distant users to gain remote access to a computer), and myriad other information. Much of this information is not readily accessible, and can only be recovered with specialized software. When it comes to potential defenses, the pictures (really "image files," that may themselves be incomplete or fragmented) are largely secondary to other data that may be found on the computer. For example,

a critical issue in a pornography possession case may be the “location” where the image files were stored on a hard drive, since computers frequently download and save images from the Internet without the user’s knowledge in “temporary” files or “caches.” See Ty E. Howard, *Don’t Cache out Your Case: Prosecuting Child Pornography Possession Law Based on Images Located in Temporary Internet Files*, 19 Berkeley Tech L.J. 1227 (Fall 2004). For these reasons, the former director of the FBI’s Regional Computer Forensics Laboratory Program has observed that “analysis of a computer hard drive takes as much time as the analyst has to give it.” Kerr, *supra* at 544; see also *id.* at 542 (“Computer hard drives sold in 2005 generally have storage capacities of about eighty gigabytes, roughly equivalent to forty million pages of text”).

This conclusion is illustrated by a recent federal case in which the defendant was charged with receiving Internet pornography. In *United States v. Lee*,⁴ the prosecution alleged that the defendant had visited child pornography web sites and saved hundreds of pictures from those sites on

⁴ *United States v. Lee*, CR04-5281RBL (W.D. Wa. 2005). Since acquittals, dismissals and reduced charges are not reported, it is often difficult for appellate courts to get a sense of just how critical it is for defense counsel to have access to the evidence against a client. The *Lee* case is a good, but hardly unique, example of how liberal discovery rules help ensure a just result in criminal cases.

his computer. At first glance the case seemed straightforward. There was no dispute that the pictures found on the computer were child pornography and the computer's Internet "history" revealed numerous visits to child pornography sites. The prosecution nevertheless did not challenge the defense's request for a copy of the hard drive and provided one pursuant to a stipulated protective order that prescribed how the copy would be handled and secured. *See* Sec. IV, *infra*. As a result of evidence uncovered by the defense's computer expert, a jury acquitted the defendant of five counts of receiving pornography.

The prosecution in *Lee* had done a limited forensic analysis of the hard drive and disclosed its expert's reports, but that expert had not noted the many viruses on the computer. These viruses included two that were specifically designed to generate "pop-up" advertisements, and a third "Trojan" virus that allowed other people on the Internet to access Lee's computer without his knowledge.⁵ Hours of research was required to identify the viruses, since thousands of viruses have been catalogued and

⁵"Pop-up" pages appear as unsolicited screens that open on the user's monitor when connected to the Internet. As one pop-up closes another automatically opens, and a dozen or more may appear in such rapid succession that the computer freezes. A single pop-up page may contain 50 or more small pictures, all of which will be automatically downloaded to the computer hard drive in a matter of seconds.

new ones appear all the time. The defense expert also reconstructed most of the Internet history recorded on the computer and found that pornography sites appeared only *after* the viruses had infected the computer. The defense's analysis further revealed that all the contraband pictures had been part of unsolicited pop-up ads for pornography sites that had been automatically downloaded as a result of virus activity. The prosecution was either unaware of or failed to disclose all of this evidence.

More than 50 hours of forensic analysis was required to develop this evidence and it would have been impossible to do so under the type of restrictions advocated by the State in the instant cases. As fully explained in the attached affidavit by Marcus Lawson, a former Customs Service and Secret Service agent and computer expert, "the computer forensics process takes considerable time and can not be done with any stated time constraints as it is impossible to know beforehand the extent of the number and size of files available which may confirm or deny the allegations."

App. A. at 8.

Law enforcement agencies typically limit their work on computer evidence to locating suspect image files and, perhaps, looking at the Internet browsing history to see what type of web sites the defendant may

have visited. *See id.* at 9. These inquiries involve limited data recovery, since investigators are looking for information, like recent Internet history, that is readily accessible. Even so, police and prosecutors routinely state in warrant affidavits seeking seizure of a computer that it is impractical to undertake even simple data recovery outside a computer lab. By contrast, defense experts have to take a much more comprehensive approach, as demonstrated by the *Lee* case. In many cases, critical data has been deleted or “overwritten,” and specialized software is required to recover the data and piece together fragments of code to reconstruct entire files. All of this analysis must be done without interference or observation by law enforcement agents, in order to preserve the work-product privilege. *See generally Knellinger*, 2007 WL 219984 at *5-6 (discussing the equipment, time and confidentiality that is required for forensic analysis by the defense).⁶

⁶ Computer forensics is also a dynamic process, in which testing and analysis evolve as trial strategies change. Thus, in the *Lee* case, the prosecution revised its theory of the case after learning of the virus activity by notifying the defense that an “expert” would testify that child pornography sites are secretive and therefore do not disseminate pop-up ads. This opinion, disclosed on the eve of trial, forced the defense to go even further in its analysis for a refutation. The defense was able to reconstruct several of the ad pages that had appeared on the defendant’s computer, clearly soliciting subscriptions to child pornography sites and containing dozens of images. The defense was able to challenge the prosecution’s theory in this manner only because the defense expert had ongoing access to the computer data and was able to address new evidentiary issues as they arose.

Given the realities of trial preparation, the State's position that it should not be required to provide copies of protected evidence to the defense, even in a case involving a computer, effectively asks the Court to grant the prosecution overwhelming advantages when preparing for trial. This Court, however, has long held that "the route of discovery should ordinarily be considered somewhat in the nature of a two way street," with trial courts "neither according to one party an unfair advantage nor placing the other at a disadvantage." *State v. Boehme*, 71 Wash. 2d 621, 632-33, 430 P.2d 527 (1967); *see also Wardius v. Oregon*, 412 U.S. 470, 475 (1973) (same). With that principle in mind, the real issue in the instant cases may not be whether the defense is entitled to copies of the prosecution's evidence for independent analysis. Instead, the more pertinent issue may be the procedures that should be used to ensure that the evidence is handled properly.

IV. REASONABLE AND EFFECTIVE "PROTECTIVE ORDERS" HAVE BEEN USED BY BOTH FEDERAL AND WASHINGTON COURTS.

The United States Department of Justice (DOJ) has recognized that the defense must be afforded "reasonable access" to "protected" evidence in child pornography cases, and that this includes providing the defense

with its own copies of all “protected material” for independent examination. *See* App. B at 2, ¶ 3 (sample stipulated protective order from U.S. District Court, Western District of Washington); *see also id.* at ¶ 2.2 (Protected material means “any information, document, or tangible thing,” including digital media, that “may contain or reference child pornography”). To this end, DOJ and federal defendants have entered into stipulated protective orders to ensure that the evidence is handled properly. *See also* App. A (Lawson Aff.) at 11-13 (listing numerous other jurisdictions that have used similar protective orders). Similarly, the State has repeatedly entered into protective orders for disclosure in child pornography cases. *See* Apps. C-F. Amici is not aware of a single instance in which a protective order has been violated or prosecutors have complained that evidence was mishandled. Nor has the State offered any reason to believe that protective orders have proven risky or inadequate.

The protective orders themselves are comprehensive in their safeguards. For example, the federal orders limit disclosure to defense counsel, one outside “consultant or expert,” an investigator, and “persons designated as trial witnesses to the extent reasonably necessary in preparing to testify.” App. B at 3-4. Each of these people must sign an

agreement that is filed with the court, acknowledging that they will abide by the terms of the order and “subject themselves to the jurisdiction” of the court if they do not abide by the terms of the order. Further, all analysis of the evidence “shall be done in a confined and secure environment which shall be inaccessible” to unauthorized individuals, no additional copies of the evidence can be produced, and any computers used to examine the evidence cannot have Internet access. *See id.* at 5-6. Numerous other stipulations apply, all of which have proven to be both workable and sufficient.

The State contends that things have changed for federal prosecutors, at least, and they are no longer required to provide copies of “protected material” as a result of the Adam Walsh Act. *See State’s Statement in Giles* at 6; 18 U.S.C. §3509m. Relying on the Act’s new discovery provisions, the State suggests that this Court should curtail discovery in child pornography cases. The State, however, misunderstands the legislation, which requires federal prosecutors to make protected evidence “reasonably available” to the defense. As one federal court has recently held, protected material may be “reasonably available” only when the defense is provided with a copy of a defendant’s hard drive and is able

to conduct an independent forensic analysis. *See Knellinger*, 2007 WL 219984 at *4.

More specifically, the Adam Walsh act provides that courts shall deny any request by the defense to copy protected material “so long as the Government makes the property or material reasonably available to the defendant.” 18 U.S.C. § 3509m(2)(A). The statute goes on to state that evidence is reasonably available if the Government provides “ample opportunity” for the defendant, her attorney and defense experts to inspect and examine the material at a “Government facility.” 18 U.S.C. § 3509m(2)(B). “While the statute does not define ‘ample opportunity,’ that term must be read to include at least every opportunity for inspection, viewing and examination required by the Constitution,” and in some cases will “include greater access than what the Constitution alone would require.” *Knellinger*, 2007 WL 219984 at *4. Based on the testimony of the defense’s experts in *Knellinger*, the court concluded that the Government’s offer to allow them to examine the computer evidence in a private room at an FBI office was inadequate and ordered the prosecution to produce and turn over, pursuant to a protective order, an exact copy of the hard drive. *Id.* at *5, 8.

Given the Adam Walsh Act's recognition that the defense must be afforded ample opportunity to examine evidence in child pornography cases, and the realities of what constitutes ample opportunity to prepare a defense in many of those cases, the State's reliance on the act to argue against full disclosure is misplaced. Instead federal courts, like courts everywhere, continue to recognize that "the rules of discovery are designed to enhance the search for truth in both civil and criminal litigation." *State v. Pawlyk*, 115 Wash. 2d 457, 471, 800 P.2d 338 (1990) (citations omitted). That search is best served by allowing both parties in a criminal case broad discovery and equal opportunities to prepare for trial. Conversely, the search is fundamentally compromised if the prosecution is allowed unlimited access to critical evidence while the defense is effectively prevented from thoroughly examining the same evidence.

When it comes to pornography cases, most trial courts have long struck a reasonable balance by affording defendants copies of sensitive evidence under strict but not unduly restrictive conditions that allow for thorough and independent examination. Since the State has not cited a single instance in which those procedures have resulted in the improper handling or distribution of the evidence, it offers no credible reason to

believe that more is required. And, to the extent that greater limitations on discovery will inevitably trench on a defendant's fundamental trial rights, the type of restrictions advocated by the State are unconstitutional.

V. CONCLUSION

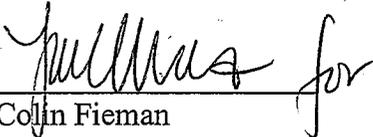
For these reasons, the Court should affirm the protective order in *Giles* and *Wear*, and order the trial court to compel the disclosure of the requested discovery in *Boyd* contingent on the State having an opportunity to seek a protective order. In the alternative, should this Court determine the record is insufficient for it to make a determination at this point, it should remand to the trial courts and allow the parties to present additional evidence.

DATED this 9th day of February, 2007.

Respectfully submitted,



Sheryl Gordon McCloud
WSBA No. 16709
Attorney for Amicus NACDL



Collin Fieman
Georgia Bar No. 259690
Attorney for Amicus WACDL



Laura E. Mate
WSBA No. 28637
Attorney for Amicus WACDL

CERTIFICATE OF SERVICE

I certify that on the 9th day of February, 2007, a true and correct copy of the foregoing BRIEF AMICUS CURIAE OF WASHINGTON ASSOCIATION OF CRIMINAL DEFENSE LAWYERS was served upon the following individuals by depositing same in the United States Mail, first class, postage prepaid:

Barbara L. Corey
Attorney for Petitioner Michael Allan Boyd
901 S. I St., Suite 201
Tacoma, WA 98405

Michael Schwartz
Attorney for Respondent Lee Giles
524 Tacoma Ave. S.
Tacoma, WA 98402

Mary K. High
Attorney for Respondent Maureen Elizabeth Wear
949 Market St., Suite 334
Tacoma, WA 98402

Gerald R. Horne
Pierce County Prosecuting Attorney
Kathleen Proctor
Pierce County Prosecutor's Office
Hugh Birgenheier
Pierce County Prosecutor's Office
930 Tacoma Ave. S., Rm. 946
Tacoma, WA 98402
Counsel of Record for the State



Sheryl Gordon McCloud

No. 793719

IN THE SUPREME COURT
OF THE STATE OF WASHINGTON

STATE OF WASHINGTON,

Petitioner/Respondent,

v.

MICHAEL ALLAN BOYD, Petitioner,

LEE GILES, Respondent,

MAUREEN ELIZABETH WEAR, Respondent

BRIEF *AMICUS CURIAE*
OF
WASHINGTON ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE
LAWYERS

Sheryl Gordon McCloud
WSBA No. 16709
Law Offices of Sheryl Gordon
McCloud
710 Cherry Street
Seattle, WA 98104-1925
(206) 224-8777
Attorney for Amicus NACDL

Colin Fieman
Georgia Bar No. 259690
1331 Broadway, Suite 400
Tacoma, Washington 98402
(253) 593-6710
Attorney for Amicus WACDL

Laura E. Mate
WSBA No. 28637
1601 Fifth Ave., Suite 700
Seattle, WA 98101
(206) 553-1100
Attorney for Amicus WACDL

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	ii
I. INTRODUCTION	1
II. A DEFENDANT’S FUNDAMENTAL RIGHT TO INDEPENDENTLY EXAMINE THE EVIDENCE AGAINST HER	5
III. THE CRITICAL NEED FOR INDEPENDENT FORENSIC ANALYSIS IN COMPUTER CASES	10
IV. REASONABLE AND EFFECTIVE “PROTECTIVE ORDERS” HAVE BEEN USED BY BOTH FEDERAL AND WASHINGTON COURTS.	15
V. CONCLUSION	20

App. A

AFFIDAVIT OF MARCUS LAWSON

I, Marcus Lawson, President of Global CompuSearch LLC, do hereby depose and state:

Background

1. I am the President of Global CompuSearch LLC, located in Spokane, Washington and have been so employed since July of 2000. Global CompuSearch LLC provides consulting, computer forensics and training services on legal issues related to computers and the Internet. The consulting work the company provides offers a special emphasis on sex crimes, child sexual abuse and child pornography issues involving the Internet.
2. Prior to my work at Global CompuSearch I was employed as a Special Agent with the United States Customs Service for twelve years. Previous to my employment with the Customs Service, I was employed as a Special Agent with both the Drug Enforcement Administration and U.S. Secret Service for five years. My education consists of a Bachelor of Science Degree in Administration of Justice from Portland State University and a Juris Doctor from Pepperdine University School of Law. During my employment with the United States Customs Service I investigated and worked as an undercover operative in cases of fraud, narcotics, weapons violations, terrorism and child pornography. For eleven of the twelve years I was a Special Agent with the Customs Service I specialized in the investigation of child pornography and child sexual abuse cases.
3. During my employment with the Customs Service I both received and provided extensive training in the areas of child pornography, the sexual abuse of children, and the behavior of pedophiles. I received training from the Customs Service, the United States Department of Justice, and other federal, state and local law enforcement agencies. I received instruction on investigations of child sexual exploitation from the Customs Service as well as training in the use of computers to obtain and distribute child pornography both from the Customs Service and SEARCH, The National Consortium for Justice Information and Statistics, Sacramento, California. I personally coordinated the Northwest Child Exploitation Conference on behalf of the Customs Service and served as an instructor in undercover techniques and case studies in the field of child exploitation and child pornography crimes. During my period of employment with United States Customs, I coordinated training seminars and trained at seminars coordinated by others, training federal, state and local law enforcement personnel in Oregon, Washington, Idaho, California, Utah, Montana, Alaska, Indiana and Michigan, the United States Attorneys Office, the Federal Public Defenders Office, the American Probation and Parole Officers Association, the Naval Investigative Service, the Federal Bureau of Investigation, the United States Postal Inspection Service, the United States Customs Service Cyber Smuggling Center and dozens of social service providers and community service groups.
4. In 1996 I created one of the first investigative manuals in use by law enforcement investigators and prosecutors outlining investigative techniques and strategies on the Internet. I assisted in the planning and creation of the U.S. Customs Cyber Smuggling Center in 1997.

I have also testified before the Oregon State Legislature on issues pertaining to the drafting of child pornography legislation. During my period of employment with the Customs Service I represented U.S. Customs child pornography investigative efforts in numerous print media and television interviews including NBC Nightly News, The Montel Williams Show and BBC Television.

5. During my employment with the United States Customs Service I personally coordinated four undercover child pornography sting operations and initiated child pornography and/or child exploitation investigations throughout the United States and the world. I coordinated these types of investigations with the Royal Canadian Mounted Police, Scotland Yard, the German Polizei, Naval Investigative Service, Army Criminal Intelligence Division, the Federal Bureau of Investigations and scores of state and local police agencies.
6. As President of Global CompuSearch, I continue to receive requests by both law enforcement and criminal defense entities for training on computer crime issues. As a result, since leaving the employ of the government, I have conducted training with sheriffs departments, police departments, state and federal parole officers associations, state and federal public defenders, state and federal public defenders investigators and private citizens groups.
7. As President of Global CompuSearch, I continue to investigate allegations of Internet crime. Since becoming a private consultant I have conducted examinations on well over two hundred computer hard drives and hundreds of other pieces of digital media, advising attorneys on findings and often comparing these findings with the reports of law enforcement forensics investigators.
8. I am also the head supervisor for Global CompuSearch and as such, review the findings and reports of all other forensics examiners employed by Global CompuSearch.
9. I am a Board Member (International Membership) of the IISFA (International Information Systems Forensics Association) and a Certified Information Forensics Investigator (CIFI). I have been recognized as a state, federal and international expert witness in the following areas: Internet undercover techniques, Internet child exploitation investigations, computer evidence in Internet investigations, pedophiles and pedophile behavior.
10. Global CompuSearch is an independent consulting firm and while the case load consists of many criminal defense issues, forensic examiners at Global CompuSearch do not act as defense advocates but rather act as factual advisors to the attorneys in these cases. Global CompuSearch forensic examiners report all findings to the attorneys regardless of whether those findings are inculpatory or exculpatory toward the attorney's client.
11. This firm's list of clients in these matters includes the United States Army, The United States Navy, The United States Air Force, The United States Marine Corps, Federal and State Public Defender Offices throughout the United States, private attorneys throughout the United States, Europe, and business entities throughout the United States and Europe. Global CompuSearch examiners have examined computer evidence in allegations of capital homicide, rape, child pornography, "traveling" for sex with minors, unauthorized access

(hacking), arson, espionage and a host of other issues. Global CompuSearch forensics examiners regularly testify about their findings in courts throughout the United States and around the world.

12. The term "child pornography," as used in this declaration refers to visual depictions of minors engaged in sexually explicit conduct. The terms "minor," "sexually explicit conduct," "visual depiction," and "production," as used in this affidavit, are defined in Title 18, United States Code, Section 2256, et sea. The term "computer", as used herein, is defined in Title 18, United States Code, Section 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."

History

13. Global CompuSearch was requested by Attorney I. Defend You to conduct a computer forensics analysis of computer hard drives and related media and to advise in the preparation of the defense in the case of the United States vs. I. M. In trouble. I have reviewed the Affidavit for Search Warrant of Special Agent You R. Caught, provided to Attorney I. Defend You in discovery in this case.
14. Attorney Defend You informed me that the prosecution has indicated an intent to oppose the defendant's request for discovery and production of mirrored hard drives and duplicated computer media because of the passage of H.R. 4472, the Adam Walsh Child Protection and Safety Act of 2006. Specifically, Sec. 504 of that act which proposes to prevent defense counsel from temporarily obtaining mirror copies of digital media in preparation for trial when it contains images alleged by the government to be child pornography provided the government provides "reasonable access" to the media at government proscribed facilities.
15. It is anticipated that I, or an investigator from my firm, would need to access the drive repeatedly to assist in the preparation of cross examination and/or possible testimony on his part as an expert witness for the defense.

The Forensics Process

16. The examination and review of computer digital evidence is unlike any other type of evidence examination. It almost always involves the review of enormous amounts of data and often requires the use of multiple forensics tools to do so. **In paragraph 36 of the Affidavit for Search Warrant authored by Special Agent You R. Caught in the instant case, he makes the following sworn statement**

"Based upon your Affiants training and experience, consultation with experts in computer searches, and your Affiants communications with other law enforcement agents who have been involved in the search of computers and retrieval of data from computer systems, your Affiant knows that searching and seizing information from computers often requires agents to seize all electronic storage devices (along with related peripherals, software, documentation, data security

devices and passwords) so that a **qualified computer expert in a laboratory or other controlled environment can more accurately analyze such evidence.** This is true because of the following:

A. Volume of evidence: Computer storage devices ... can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence by storing it in random order with deceptive file names or deceptive file extensions. **This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks to months,** depending on the volume of data stored. **It would also be impractical to attempt this type of data search on site.**

B. Technical requirements: **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 is qualified to analyze the system and its data.** In any event, data search protocols are exacting scientific procedures 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 inadvertent or intentional modification or destruction ... **a controlled environment is essential to its complete and accurate analysis.**" (emphasis mine)

17. In a recent case handled by Global CompuSearch, the Texas Court of Appeals found reversible error when the State refused to provide a mirror copy of the defendant's hard drive for independent review, stating;

"In so holding, we disagree with the State's position that such a review must be conducted at a State-controlled facility. We would not require a chemist to take a "porta lab" with him or her into an evidence room to check alleged contraband drugs, and it is not appropriate to require a computer expert to carry his or her equipment into a State facility to review the documents." Taylor v. Texas (2002) WL 31318065.

18. Another recent child pornography case handled by this office was United States vs. Hill 322 F.Supp.2d 1081 (C.D.Cal. 06/17/2004). In a written opinion of Judge Alex Kozinski ruling in favor of a defense motion for discovery but discounting a defense contention that the law enforcement agents in that case should have done an "on-site" examination, he states;

"Even if the police were to bring with them a properly equipped computer, and someone competent to operate it, using it would pose two significant problems. ... Second, the process of searching the files at the scene can take a long time. To be certain that the medium in question does not contain any seizable material, the officers would have to examine every one of what may be thousands of files on a disk — a process that could take many hours and perhaps days. See pages 23-24 infra. Taking that much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive. ... "

19. Continuing in the opinion, Judge Kozinski went on to rule the defense, and specifically Global CompuSearch was entitled to mirror copies of the computer media containing contraband;

"Defendant wishes to obtain two "mirror image" copies of the computer media analyzed by the government's expert to allow his own expert to conduct a forensic analysis and his counsel to prepare his defense. The government opposes producing these items, offering instead to permit the defense to view the media in an FBI office and to conduct its analysis in the government's lab.

Federal Rule of Criminal Procedure 16(a)(1)(E) provides:

Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant.

Rule 16 clearly covers the items defendant has requested. They are "data, photographs, [and/or] tangible objects" within the government's possession. Moreover, they are material to the preparation of the defense, the government intends to use them in its case-in-chief and they were obtained from defendant. Rule 16(d)(1), however, allows the court to regulate discovery: "At any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief."

The government argues that since child pornography is contraband, defense counsel and his expert should be required to examine the images in the controlled environment of the government facility. The cases cited by the government, though, all involve appeals from district court decisions denying a defendant's motion to compel production. They do not hold that a district court would abuse its discretion if it were to order the government to produce copies of the materials.

The government analogizes the zip disks to narcotics, arguing that their inspection and analysis by defendant's expert should take place in the government's lab under government supervision. This analogy is inapt. Analysis of a narcotics sample is a fairly straightforward, one-time event, while a thorough examination of the thousands of images on the zip disks will take hours, even days, of careful inspection and will require the ability to refer back to the images as the need arises.

The court concludes that defendant will be seriously prejudiced if his expert and counsel do not have copies of the materials. Defense counsel has represented that he will have to conduct an in-depth analysis of the storage media in order to explore whether and when the various images were viewed, how and when the images were downloaded and other issues relevant to both guilt and sentencing. The court is persuaded that counsel cannot be expected to provide defendant with competent representation unless counsel

and his expert have ready access to the materials that will be the heart of the government's case.

The government's proposed alternative — permitting the defense expert to analyze the media in the government's lab at scheduled times, in the presence of a government agent — is inadequate. The defense expert needs to use his own tools in his own lab. And, he cannot be expected to complete his entire forensic analysis in one visit to the FBI lab. It took defense counsel between two and three hours to quickly scroll through the 2,300 images in the Encase report, so it is likely to take the expert much longer than that to conduct a thorough analysis. **Defendant's expert is located in another state, and requiring him to travel repeatedly between his office and the government's lab — and obtain permission each time he does so — is unreasonably burdensome.** Moreover, not only does defendant's expert need to view the images, his lawyer also needs repeated access to the evidence in preparing for trial.

There is no indication that defendant's counsel or expert cannot be trusted with the material. The expert is a former government agent who has a safe in his office and has undertaken to abide by any conditions the court places on his possession of the materials. He has experience in dealing with child pornography and takes precautions to ensure that contamination doesn't occur, including using the Encase software and fully "wiping" the forensic computers on which he examines the images. Defense counsel is a respected member of the bar of this court and that of the Ninth Circuit. The court has every confidence that he can be trusted with access to these materials. [Emphasis mine]

20. The resulting court order reproduced in the opinion states;

“2. The government shall provide defendant's expert, Marcus K. Lawson of Global CompuSearch, LLC, a copy of all of the Encase evidence files relating to this case, which includes evidence files for all media seized from [address deleted] on April 6, 2000, necessarily including any and all actual or alleged child pornography and/or contraband contained thereon. Mr. Lawson shall maintain and secure the Encase evidence files in the following manner:

a. Copies of the Encase evidence files shall be maintained by Mr. Lawson in accordance with this Order, and shall be used by Mr. Lawson solely and exclusively in connection with this case.

b. Copies of the Encase evidence files shall be maintained by Mr. Lawson in a locked safe in the offices of Global CompuSearch, LLC at all times, except while being actively utilized as provided for in this Order.

c. A copy of this Order shall be kept with the copies of the Encase evidence files at all times.

d. Copies of the Encase evidence files shall be accessed and viewed only by Mr. Lawson and staff employed by Global CompuSearch, LLC who Mr. Lawson has given this Order to and who agree to be bound by the requirements of this protective order.

e. Mr. Lawson shall maintain custody over the Encase evidence files and shall maintain a list of all Global CompuSearch, LLC employees granted access to the Encase evidence files.

f. Any computer into which copies of the Encase evidence files may be inserted for access and operation shall not be connected to a network while a copy of the Encase evidence files is inserted into any computer.

g. The computer into which copies of the Encase evidence files are inserted may be connected to a printer only under the following conditions: that any printer utilized is a local printer, that the printer may be connected only when and as necessary to print non-graphic image files, and that Marcus Lawson or staff employed by Global CompuSearch who are subject to this Order shall be personally present at all times a printer is connected.

h. In no event shall any graphic image containing actual or alleged child pornography be copied, duplicated, or replicated, in whole or in part, including duplication onto any external media.

3. Within 30 days of termination of this matter (including the termination of any appeal), defense counsel shall return (or cause the return of) copies of the retained computer evidence and the Encase evidence files to Special Agent Tim Alon or a representative of the Federal Bureau of Investigation. Upon the return of the copies of retained evidence and the Encase evidence files, defense counsel shall file a brief report to the Court specifying that the terms of this Order have been complied with and reporting the return of the copies of evidence.

IT IS SO ORDERED.”

21. Just as discussed in the Hill opinion by Judge Kozinski, **and just as expressed in Agent Caught's own sworn Affidavit for Search Warrant in this case**, in order to assist Attorney Defend You in his preparation of the defense of Mr. Trouble, it is likely to take me or an examiner from my office many hours to do even a preliminary analysis of the data found in the hard drive belonging to Mr. Trouble and will take him several more days of analysis to help prepare Attorney Defend You for Mr. Trouble's trial. Without a repeated on-going, as needed access to Mr. Trouble's media, it simply is not possible for my firm to properly assist Attorney Defend You in preparing for Mr. Trouble's trial.
22. In cases involving allegations of criminal misconduct, computer evidence is examined by law enforcement examiners, as was done here. It is the job of these police examiners to forensically examine the computer evidence given them looking for, and documenting, evidence of the criminal violation. Rarely (if ever) do police technicians examine this same

evidence for exculpatory data that would assist the defense. Rather, if such evidence exists, it is deemed the responsibility of the defense team to find and document it. This is the investigative process of digital forensics.

23. Because computer evidence is by definition digital, and digital evidence is fragile, such evidence requires special forensics software tools for examination as well as the knowledge of how to use them correctly. Hence, computer evidence is virtually always examined in a controlled laboratory environment by trained personnel using specialized investigative software. Global CompuSearch has such a laboratory with a wide variety of forensic software available to its examiners, an up-to-date technical library, and different hardware computer components for every operating system available as well as the combined technical knowledge of the four examiners employed here.
24. I can state from repeated experience that it is vitally important for the defense team to have the same access to the evidence in this case that the prosecution team has had and continues to have. As noted by Judge Kozinski and **as stated in the Affidavit for Search Warrant in this very case prepared by Agent Caught**, virtually every affidavit for search warrant filed by law enforcement officials seeking search warrants for computer related evidence, the computer forensics process takes considerable time and can not be done with any stated time constraints as it is impossible to know beforehand the extent of the number and size of files available which may confirm or deny the allegations.
25. The standard of thoroughness in the examination process that Global CompuSearch examiners are required to maintain often requires the use of multiple forensics tools. These tools may be of a software or hardware nature. Some software is more useful for thoroughly examining specific areas of the computer than others. Sometimes a forensics program proves more appropriate for recovering text dialog than for recovering graphic images and another graphic-image program might recover specific files from specific locations in the computer better than another. In other words, the examination of computer data for evidentiary purposes is a dynamic process requiring multiple tools and substantial time and it is unreasonable to expect any competent computer examiner to bring his/her entire forensics laboratory including every software possibly needed and every computer hardware component possibly needed to a government proscribed location and then complete a detailed, thorough examination of the computer media under any kind of time constraint that would be financially and practically reasonable. In the course of the exam in this case it will likely be necessary to use multiple forensics software or other tools available in Global CompuSearch's laboratory which would be unavailable in a police controlled environment.
26. In the instant case, images have been alleged by the government to be visual depictions of minors in sexually explicit poses, in violation of federal law. Three issues that Global examiners take into consideration in all child pornography cases are:
 1. Whether the charged images do indeed meet the legal criteria for obscenity and/or child pornography.

2. Whether their location within the computers hard drive tends to indicate a knowing possession by the defendant.
 3. The original source of the images and the context of their download.
27. Although not the only issues to be examined, these three issues in particular require personal observation of the drives themselves. Thus, independent examiners are required to examine not just the images themselves, but more importantly;
- Their origination point from the Internet
 - Their path through the operating system to their present location
 - Their file date/time stamps which may or may not link specific computer use to the defendant or others.
28. Much of what passes as “computer forensics” in law enforcement entities devoted only to data recovery, is not investigative in nature at all. A field investigator sends these entities a seized computer. The technician at the facility makes a copy of the media and then extracts what the investigator asks them to extract. Little and often no investigative effort goes into the analysis of the seized drive.
29. Data recovery is the initial step in a computer investigation. The media needs to be copied correctly to ensure that a duplicate is created. Once that copy is created, it is up to the investigator to determine what evidence it contains. This is where the distinction begins. Many police computer forensics labs this firm has dealt with (and we have dealt with labs all over the country) will extract what the case agent or detective asks them to extract. In child pornography cases, this is usually limited to the suspect images and perhaps the Internet history files (which show world wide web browsing activity). This information is copied out and placed on CD Rom and given to the investigator.
30. In the experience of this firm, this approach usually leads to overlooked evidence, many times even overlooked evidence that would be extremely important to the prosecution of the case. While a layman might conclude that the technician extracting the data is performing “computer forensics”, in actuality, all they have done is data recovery.
31. Computer forensics, at least as that term is applied in this office, is a great deal more than this. More accurately called computer investigations, when this firm receives a piece of media to examine, we examine all aspects of the information on it and are prepared to inform our clients of everything that is potentially relevant to their case. In other words, we **investigate** the media and determine what occurred, when it occurred, how it occurred and who was responsible for its occurrence. To answer these questions requires not just a working knowledge of data recovery, but a working knowledge of the Internet, it’s applications, how offenses are committed with these applications, what types of behaviors are associated with which applications and a myriad of related issues.
32. But, in addition to that working knowledge, it also requires the ability of the examiner to be able to research new applications and programs on the fly as they are encountered during an

examination. For example doing examinations in our own laboratory gives Global CompuSearch examiners live Internet access to research a new program or application. Similarly, doing exams in our laboratory gives these examiners access to our technical library as well as the expertise of other examiners to rely on to solve examination problems. The firm's laboratory also has test "mule" computers running various operating systems (Macintosh, Linux, and various versions of Windows) so that a new application or program can be run on the same operating system is use on the defendant's machine to determine the nuances of how it works. It is simply a fact that various versions of various Internet applications and programs run differently, store data differently and react with the user differently depending not just on what operating system is used (Macintosh/Windows/Linux) but the different versions of those operating systems. None of these things are available in a government controlled facility nor would it be even remotely possible to bring these investigative tools to one.

33. For the government to assert that these types of resources can all be "loaded onto a laptop" and brought to a government office (as I was told recently by one federal agent) is either very naive or shows a lack of appreciation of what computer forensics actually entails. In reality what such an approach does is severely limit this firm's ability to know everything we need to know about a case, something the government is quick to exploit in the court room.
34. In the instant case, my firm's inability to have complete access to the media will prevent me or a forensic investigator from my firm from testifying as an expert should Attorney Defend You wish him to do so simply because we will not have been able to prepare ourselves with the knowledge of the defendant's hard drive we would need to not just testify effectively for Attorney Defend You but to withstand cross examination. Cross examination that will, no doubt, be assisted by a government agent that has had weeks of access, including access right up to the time of cross examination.
35. This type of thorough analysis is the same for every case this office handles. More than just our reputation, individuals liberties (and in some cases their lives) are at risk if we make mistakes or miss important evidence. The resources this firm has acquired, such as our test mule machines with various operating systems, have been acquired because they showed themselves repeatedly necessary for us to offer sound opinions to our clients. As a private firm, dependant on making a profit to survive, we have not acquired these expensive investigative tools lightly, rather, they are acquired because we need them to effectively perform our services. And, again, to believe that these types of assets can be "loaded onto a laptop" and carted around the country to various government facilities is simply not realistic.

The Allegation of Child Pornography

36. An important issue that should be noted is that it is merely the **allegation** that images are child pornography that triggers the act and its consequential restrictive access to discovery. In the six years that this firm has been in business and consulting on these types of offenses, this office has had numerous cases where the images alleged as child pornography were in fact not child pornography at all. In a federal case handled by my office in the District of Hawaii in 2002, United States v. Thomas Schnepfer, for instance the government alleged

images in the defendant's computer as child pornography that were in fact images of adult pornography actress Melissa Ashley. This mistaken allegation triggered the necessity of a federal court order and my office received a copy of the defendant's hard drive. My firm's examination revealed that the images in question were not child pornography but actually Ms. Ashley yet even when the government was provided this information the child pornography allegations were not dropped necessitating Ms. Ashley's presence in court to testify regarding her identity in the images and her age. The child pornography charges were subsequently dismissed by the court, not the government.

37. Similar scenarios have occurred on other occasions with this firm, particularly where the allegation of child pornography is used by the government to bolster other (non pornography) charges against the defendant. The allegation of child pornography possession is used to "paint" the defendant as a deviant child predator to increase the odds of conviction when in reality, the images being used to do so are either not pornographic in nature (using current legal standards as related in U.S. v Dost) or, as was the case with defendant Schnepfer in Hawaii District Court, are actually of persons of legal age. In either scenario, it is the mere **allegation** that the images are child pornography that triggers this restrictive access to discovery and, in the experience of this firm, it would be naive to believe that the government does not take advantage of that fact at the defendant's expense.

Previous Orders

38. This firm has been asked to address these issues and perform independent examinations of hard drives containing child pornography in numerous cases throughout the United States. The list of criminal cases below represents a portion of child pornography prosecutions wherein this firm was tasked via court order with the independent examination of hard drives containing child pornography at our laboratory facility. These examinations were done in Global CompuSearch's lab, independent of any prosecutorial or law enforcement presence and were safely and properly handled in every case:

- AZ v Jason Donald Simpson CR2003-019335-001 DT
- AZ v Craig Charles Rose # 2 CR2002-012446
- CA v Christian Kacher YA 049747
- CA v David Westerfield SCD165805
- CA v John Scott McClintock SCD162444
- CA v Kendell T. Ontko M01910070-2
- CA v Kurtis Brinkerhoff VCR168128
- CA v Roman Montiel FC-196731
- CA v Kenneth Williams F12750
- CA v Robert Pflieger GJ21408
- CO v Peter K. Dunn 02 CR 5218
- CO v Michael Gretzy 03CR2459
- CT v George Russell CR01-74313
- IL v Timothy Noonan 04 cf 3381
- MA v Randolph Roberge 0167 CR 2089

- MA v Richard Landau 2002-286-001/005
- NE v Samuel Thompson CR03-163
- NJ v Peter DiGiovanni 05-0300047-S
- NJ v Sean Fitzgerald 01-1944
- NY v Alexander Bueno-Edwards 03-1106
- NY v Brian Manzulo 203-2002
- NY v Warren Seper 03-0869
- OR v Steven Eric Gelhardt 0003613CR
- OR v David Waterstreet CR0400506 / 05-MC-9101
- US v Anthony Donadio CR03-40007
- US v Dennis Peterson CR01-5294FDD
- US v Chance Rearden CR 01-825-SVW
- US v SSgt E. Goodin US Court Marshall
- US v Droeder US Court Marshall
- US v Handel US Court Marshall
- US v A1C Howard US Court Marshall
- US v TSgt Fields US Court Marshall
- US v Bryan A. Nash Cr. S-04-0076-WBS
- US v Robert MacKenzie 03 -711 (JEI)
- US v Billy Smith 4:04 CR 141 SNL
- US v Justin Barrett Hill CR 02-1289-AK
- US v A1C Charles R. Phillips US Court Marshall
- OR v Sung Koo Sim C-04-1709-CR
- US In Re: Sung Koo Kim C-04-1709-CR
- US v Anthony Alexander 04-20005-BC
- US v Paul Greiner CR03-151-BLG-RFC
- US v Floyd T. Latta US Court Marshall
- US v Humberto Castaneda Padilla CR-03-1045-MMM
- US v Miriam Lawal CR-03-66-DDP
- US v David Michael Hill CR 02-1187-DDP
- US v Fallon Woodland CR 01-2003 JF
- US v James Edward Lee CR-F-02-5301 OWW
- US v Jeffery Scott Kuzdzal CR 03-12 Erie
- US v Jeffrey Brian Zeigler CR-03-08-BU-RFC
- US v John Lester CR02-6002FDB
- US v John Olinger
- US v Kenneth Young 04-CR-351-WM
- US v Kenneth King CR02-0376L
- US v Loren Samuel Williamson CR 02-60017-AA
- US v Michael Aaron Wilson CR02-6065FDB
- US v Robert Tashbook CR 01-20160 JF
- US v SSgt David T. Puckett Order and Stipulation, 18 MAR 2003
- US v Thomas M. Schnepfer 02-00062 HG
- US v Thomas Salinas CR 01-1029-AHM

- US v Wilson-Rutan, Andrew G Order dated 29 APR 2003
- US v Tony Guerrieri Order of Stipulation CR-03-144-GF-SHE
- US v Jarod D.D. Smith US Court Marshall
- US v Ronald Mikos 02 CR 137-1
- US v Hoover
- US v Robert William Crosbie 06-00047-CG
- US v William Heiser CR-04-0270
- US v David Shumaker
- US v SrA Luis Osorio
- US v SSGT John Lazard
- US v SrA Luis Osorio
- US v Daniel Brown
- US v Camnetar
- US v A1C Howard
- US v Tsgt Fields
- US v Rangel
- US v Shane Robert Ferguson CR 05-1154-JSL
- US v Jason Bilgere CR02870ERW
- US v Shannon Duncan CRS-04-022-WBS
- US v James Cannel CR-05-2059-EFS
- US v Bernnie Russell 03CR3283-JAH
- US v Tyrone Alan Ganoe CR-06-19-DSF
- US v John Mantos 06CR1416
- US v Gregory Vanausdel CR-04-20215JW
- US v Sharyar A. Raheem
- US v Kenneth Paul Wilk 04-60216-CR-COHN/SNO
- US v Willard Wm McDonough
- US v Ronnie Gurganusje 9:04-CR-58
- WA v Harjana Kioe 03-1-00006-4
- WA v James P. Degroff 02-1-0960-7
- WA v Thomas Lee Witkoski 02-1-03514-2
- WA v William Mannikko 01-1-697-0

39. Please note that this list is a small representation of court orders allowing this firm's temporary custody of contraband media and is by no means all-inclusive. It also does not include the numerous non-child pornography criminal cases that this office handles, notably, several capital homicide cases and the prosecution of Senior Airman Al Halabi for what was originally a death penalty espionage allegation by the United States Air Force.

The Forensics Process Pre Trial

40. It has been this firm's repeated experience that in preparing for trial, the forensics examination process is dynamic on both sides. As issues are raised by both sides in the release of Rule 16 and Jenks material, the claims of either must be verified or refuted by the

experts. This can only be done by the defense if the defense expert has the ability to have repeated "as needed" access to the forensics copy of the computer media. In the investigative process described above, it is obvious why it would not be reasonable for an examiner to have to return to the government proscribed location continually throughout the dynamic process of release of discovery.

41. A government "on-site" approach also fails to consider the reality that U.S. Attorney's Offices and other government facilities are not "open" to the public and will only allow non-agency access roughly between 9:00AM and 5:00PM. When we have attempted to do "on site" examinations in the past, this invariably is an issue since we are not allowed to "come and go" from a government office. It is very rare for examiners from this office to be able to confine their examination of a given hard drive or pieces of media to specific hours between 9:00AM and 5:00PM, and it is not unusual for Global CompuSearch's examiners to be doing forensics examinations of computer media well into the night and sometimes early-morning hours, particularly in the days leading up to trial. It is also not terribly uncommon for the government to hold off providing discovery at all until just days before trial (particularly in military prosecutions) necessitating an around the clock or weekend analysis. The examiners of this firm have attempted to work with the government in the past under constraints requiring "on site" examinations and found them unworkable for both Global CompuSearch and the government.
42. In an affidavit authored by Kevin Peden of my office regarding a recent attempted on-site evaluation at the Immigration and Customs Enforcement office in San Diego (August 9, 2006) he offered the following description;

"Based on the fact that the approval came late in the work day on August 8th, I was unable to leave Spokane Washington until August 9th, 2006 in the 0600 hour. Once there I drove to Camp Pendleton to meet with Capt Slabbekorn regarding the specifics of my duties on this examination. Up until my arrival in San Diego, I was under the impression that I would be conducting the examination on Camp Pendleton. I was planning on working from 0700 hours to 2200 hours each day in an attempt to complete this hasty examination. I was later advised by the Special agent Barnes, I.C.E. that the examination would take place in San Diego at the ICE office. I was also advised that this examination would have to be supervised by a federal agent.

Based on this information, Capt Slabbekorn and I contacted SA Barnes, ICE. We were assured that the supervision was necessary but that it would not intrude on the attorney client privileges afforded to the defense in this case. Barnes stated that they would be in the room but would not be watching what I was doing in the exam. During this conversation, SA Barnes asked what I needed from them and what time I was planning on working on the exam. I explained that I would need to work till about 2200 hours each night and begin by 0700 hours each morning. SA Barnes stated that he would see what he could do and let me know. I then left Camp Pendleton and drove to the San Diego office of ICE. I arrived there at approximately 1600 hours.

Once inside, SA Barnes escorted me to a large conference room and provided space to work at a conference table. He also provided one drive to begin with. This drive had the case files of 2 of the computer drives collected in this case as well as one power strip. SA Barnes advised me that he was told that his supervisor stated that ICE would not provide supervision except for the hours of 0830 – 1700 hours. He did state that he could stay a “little longer” if needed but not to 2200 hours. He also stated that he had attempted to make arrangements to have the media moved to Camp Pendleton for the examination so that the hours for my examination could be extended. He stated that he had been informed by “the powers that be” at Camp Pendleton, that this would not be afforded to the defense and that all examination would be done in San Diego at the ICE office. This greatly reduced the time afforded to the examination process. While we were discussing the time issues, SA Barnes stated, “I don’t know what you can get done in this time, I have never done an investigation that fast”. He also stated during my investigation that he spends at least 30 hours on most examinations.

I began my examination but experienced the following issues during the exam.

- The hours which I was allowed to work on the drive was 1600 – 1900 hours on August 9 and 0830 – 1700 hours on August 10, 11, 2005. I was able to begin the exams each day roughly at 0845 to 0900 hours after parking and setup were completed. Due to the limitation in time, I took a total of two, two minute restroom breaks and no other breaks on any of the days of examination. On August 9th I stayed to around 1900 hours as SA Barnes stated that he would stay until that time. On August 10, I was able to start my exam around 0900 hours due to heavy traffic on I-5 from Oceanside to San Diego and parking issues. On August 11th, I left even earlier but found heavy traffic. I was able to start my examination around 0845 hours. I left the office on August 10 and 11 around 1700 hours. A complete investigation would have taken a week to a week and a half.
- Through the process, multiple agents were entering the room, talking to each other and on the phone. At one point I had 5 agents in the room. They were attempting to set up a computer for training uses next week. While they were in the room, one agent was roaming around near my attorney/client process to the point that I had to lock my computer several times to prevent the contents of the screen from being viewed.
- Throughout the investigation, I needed to converse with Capt Slabbekorn and my other examiners within my office but could not do so due to the supervision of ICE. Based on confidentiality issues surrounding my computer being left unattended, I felt that I needed to remain in the office at all times my computer was running. I was not in a secured office which would have afforded protection against the government reviewing it had the opportunity presented itself.

- Throughout the investigation, I needed internet access on a non-forensic computer for research. Due to the limitation of the examination area, this was not possible.
- During my investigation, several agents entered the room while I was working. They had many conversations, had paperwork spread out across a different conference and had many phone conversations. This was very distracting and made the investigation more difficult.
- During my investigation, I had case agents making phone calls to book their travel plans. This lasted nearly an hour.
- On Friday, during my investigation, Major Gleason, the prosecutor in this case arrived to check in with me on the progress of the investigation. He asked if I was going to be able to complete the investigation. I told him that I was about 18 hours into a 60 hour investigation and that there was no way a complete exam was possible under the circumstances. He relayed to me that he “sure hoped the case would not have to be continued”
- There were several times during my exam, that the supervising SA told me that I should reconsider working for the defense and come to work with the federal government.”

43. I can state from repeated experience in attempting to work with the government “on-site” that my examiner Kevin Peden’s experience is very typical. We are not provided privacy, we are not given the time we need we are not allowed to put in the hours necessary on a government time table and we do not have access to the tools we routinely need in the course of daily forensics examinations. In fact, it has been stated by agents from the Spokane ICE office that they do intend to physically observe examinations performed at their office.

44. It has been the repeated experience of Global CompuSearch examiners that when equal access is denied to the defense team, the prosecution is quick to exploit this in the courtroom and it is often presented to the fact finder as a lack of knowledge or preparation, when in reality, the defense has simply not had the same access to the media as the prosecution team.

45. These two overriding reasons, (1) the need to do examinations on our controlled, sterile and prepared machines in our own controlled laboratory environment with access to the other investigative tools present within it and (2) the continuing need to assess the media at the attorney's request in the days leading up to trial, are the primary reasons we, as a firm, made the determination that if we could not do examinations in our laboratory, we should not do them at all because to do so was a disservice to our clients and the persons they represent.

Privacy Issues

46. Another reality of an "on site" examination is that Global CompuSearch runs an active business that, as of this writing, has dozens of open cases. Our examiners routinely take calls and discuss private matters not only with the attorney whose case they may be currently examining, but with clients from literally all over the world, throughout the day, which is impossible to do when accompanied by a government agent able to overhear everything that is said.
47. In the affidavit filed by examiner Peden in my office mentioned above, he makes the following description related to his privacy during the examination process in the ICE offices in San Diego;

"Throughout the process, multiple agents were entering the room, talking to each other and on the phone. At one point I had 5 agents in the room. They were attempting to set up a computer for training uses next week. While they were in the room, one agent was roaming around near my attorney/client process to the point that I had to lock my computer several times to prevent the contents of the screen from being viewed.

Throughout the investigation, I needed to converse with Capt Slabbekorn and my other examiners within my office but could not do so due to the supervision of ICE. Based on confidentiality issues surrounding my computer being left unattended, I felt that I needed to remain in the office at all times my computer was running."

Forensic Hardware

48. A government proposal for "on-site" examination also fails to take into account the eccentricities of working with electronic media. Our examiners have several times experienced damage to their forensic computers merely by transporting them on aircraft that rendered the machine unusable once the destination was reached. The reality is that desktop forensics machines must be checked as luggage when traveling on airliners which, in our experience invariably results in hardware problems at the destination and upon return.
49. This can be extremely frustrating as it is almost always our clients who have paid for our travel and that travel is virtually always limited to a minimum number of days. When the "on-site" examiner has to spend the first day of a two day exam (bearing in mind that when working in our laboratory we estimate **30 hours** for the typical forensics exam) repairing a broken forensics machine, a competent examination becomes impossible.
50. Another reality also is that even "high tech" forensics computers sometimes refuse to work, go down and crash. When these problems occur, being separated from our Spokane office and additional forensics machines becomes a major problem.

Contraband Media Security

51. As has repeatedly been explained in declarations, testimony and in person, this office never, under any circumstances, screen-captures or reproduces child pornography (or anything even closely resembling such) at any time or for any reason. The numerous court orders which

have allowed us to possess mirror images of hard drives containing child pornography contraband have always specifically stated this, but even if they had not, this is the policy of Global CompuSearch.

52. Global CompuSearch is very familiar with the proper handling of computer evidence that has been deemed contraband. As stated above, I was previously employed with the government as a federal agent and has been entrusted with the storage and handling of child pornography evidence in child pornography/sex abuse cases on literally hundreds of occasions. I was, in fact, the assigned evidence custodian at my previous field office and the policies and procedures for evidence handling in this office have been created by me.
53. Global CompuSearch LLC specializes in the evaluation of computer evidence for litigation purposes. As such, all computer media is handled in a traditional law enforcement evidentiary manner. Global CompuSearch secures all such media in its digitally secure safes (which are located in a secured room within the office) between examinations with the appropriate court order attached. Evidence is removed from the safe only for evaluation and returned immediately upon any cessation of forensics work. As is this company's regular practice when receiving media in child pornography cases, Global CompuSearch request any drive(s) or other media to be marked by the technician making the forensics copy, the serial numbers are noted by Global CompuSearch and such drive(s) are wiped upon completion of the case, returned to law enforcement for wipe verification and a report of data destruction is provided to the attorney to file with the court.
54. As I have stated, I have been investigating child pornography crimes as either a federal agent or with my firm, Global CompuSearch, since 1989 and have seized, categorized and presented for prosecution thousands of images of child pornography going back to days even before computers to magazines and video tapes.
55. We request that evidentiary drives be shipped to our lab from the law enforcement entity making the copy (with an accompanying court order attached) via FedEx. As a firm, we have chosen FedEx for the shipping of media because of their superior package tracking system. From my prior government experience I know for a fact that government entities routinely use FedEx, UPS or DHL International for the purpose of delivering contraband media to and from other government offices. This procedure has been this firm's method of operation since our inception and this office has received and examined scores of computer hard drives containing child pornography contraband.
56. In many cases handled by Global CompuSearch, the government has previously conceded that contraband can be safely reviewed in our computer lab and a large number of court orders accompanying contraband media to our laboratory are the result of stipulations by the United States Attorneys Office and state prosecutors' offices throughout the country.
57. In those cases where release of media discovery was objected to by the government, and that media was subsequently received by this office via court order, there has *never* been an issue of loss or misuse of contraband. The orders as well provide for severe penalties should that be the case.

58. I also know from personal experience that it is not uncommon for prosecutors, including federal prosecutors to retain outside computer forensics expertise and release copies of contraband media to these experts. I am not privy to whether those releases included the government's obtaining a court order to do so.
59. I would submit that, in fact, many federal prosecutors and individuals in the Justice Department, as well as dozens of federal agents who have worked with this firm over the years are well aware that this firm is extraordinarily trust worthy with evidence.
60. Global CompuSearch prides itself, and in reality is based on, its honesty, its independence and its sensitivity to both the protection of children as well as the protection of the rights of accused persons. We inform counsel of all the facts we discover, both good and bad. This declaration is offered to the court with no other motive than to attempt to insure that both sides in these cases have equal access to the evidence in questions and arrive at the truth.
61. Again, the need to do examinations on our own forensics machines in the controlled laboratory environment of our offices including access to the other investigative tools present within it as well as the continuing need to assess the media at the attorney's request in the days leading up to trial, are the primary reasons we, as a firm, have previously made the determination that if we could not do examinations in our laboratory, we should not do them at all. We simply determined that to do examinations in any other way was a disservice to our clients and the persons they represent.

I swear under penalty of perjury that the foregoing is true.

Marcus K. Lawson
President, Global CompuSearch

DATE: _____

App. B

The Honorable Ronald B. Leighton

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



05-CR-05238-ORD

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA,

Plaintiff,

v.


Defendant.

CR05-5238RBL

STIPULATION AND
PROTECTIVE ORDER RE:
DISCOVERY OF CHILD
PORNOGRAPHY MATERIALS

The United States of America, by and through John McKay, United States Attorney for the Western District of Washington, and Vincent T. Lombardi, Assistant United States Attorney for said District; and the defendant,  ("Defendant"), and his attorney, Colin Fieman ("Defense Counsel"), hereby stipulate and agree, and on that basis seek confirmation by order of the Court, as follows:

1. Purpose. The purpose of this Protective Order is to allow Defendant's Counsel to have reasonable access to Protected Material seized from Defendant, including Media that contains Child Pornography, for the exclusive purpose of preparing a defense of Defendant in the above-captioned matter. Defendant and Defense Counsel agree that any production of Protected Material as defined herein, is governed and subject to Rule 16 of the Federal Rules of Criminal Procedure; CrR 16 of the Local Rules for the Western District of Washington; and the child victim privacy provisions of 18 U.S.C. § 3509(d). Defendant and Defense Counsel expressly recognize that any disclosure of Protected Material in violation of any term of this Protective Order will

1 | subject them to the penalties and remedies set forth in Section 9 of this Protective Order.

2 | 2. Definitions.

3 | 1. Defense Counsel. "Defense Counsel" means the counsel of record
4 | representing Defendant in the above-captioned matter, who has signed this agreement. It
5 | does not mean any other person associated with the counsel of record's firm or agency,
6 | including but not limited to other counsel and secretarial and support personnel.

7 | 2. Protected Material. "Protected Material" shall mean any
8 | information, document, or tangible thing, upon which any expression, communication,
9 | or representation has been recorded by any means, that may contain or reference Child
10 | Pornography.

11 | 3. Child Pornography. "Child Pornography" shall have the meaning
12 | given that term in Title 18, United States Code, Section 2256(8).

13 | 4. Visual Depiction. "Visual Depiction" shall have the meaning given
14 | that term in Title 18, United States Code, Section 2256(5).

15 | 5. Computer. "Computer" shall have the meaning given that term in
16 | Title 18, United States Code, Section 1030(e).

17 | 3. Production of Protected Material. The United States agrees to provide
18 | Defense Counsel with one (1) copy of all Protected Material that can be duplicated. If
19 | the Protected Media is documentary and able to be reproduced on a photocopier, the
20 | United States may elect to produce that Protected Material on paper that may not be
21 | reduplicated on a photocopier. If the Protected Material is digital media, the United
22 | States will attempt to produce bit by bit or mirror images of said media, necessarily
23 | including any and all Child Pornography and/or contraband contained thereon. In
24 | connection with the production of copies of all Protected Material, Defense Counsel will
25 | furnish the United States with non-photocopy paper and the necessary computer media
26 | onto which a mirror image of the Protected Material may be prepared.

27 | ///

28 | ///

1 4. Use of Protected Material.

2 1. General. All Protected Material produced under this Protective
3 Order is to be used solely for the purposes of this criminal proceeding and for no other
4 purpose. Persons having access to Protected Material shall not disclose or provide
5 Protected Material to any person not authorized under this Protective Order. No
6 Protected Material may be made available to, or in any manner revealed to, or discussed
7 with, any other person, except: (1) solely in accordance with the procedures set forth in
8 this Protective Order; or (2) upon Court order.

9 2. Advice of Counsel. Nothing under this Protective Order shall bar
10 or otherwise restrict Defense Counsel from rendering advice to Defendant with respect
11 to this action, and in the course thereof, relying in a general way upon examination of
12 any Protected Material. However, in rendering such advice and in otherwise
13 communicating with Defendant, Defense Counsel shall not disclose the contents of any
14 Protected Material contrary to the terms or intent of this Protective Order.

15 5. Access to Protected Material.

16 1. General. All Protected Material produced by the United States to
17 Defense Counsel, shall be maintained in a locked and secure drawer, cabinet, or safe.
18 The drawer, cabinet or safe used to secure the Protected Material shall be accessible
19 only to Defense Counsel and other persons authorized by the Protective Order.

20 2. Permissible Disclosures. Protected Material may be disclosed to
21 Defense Counsel and court officials involved in this criminal proceeding (including court
22 reporters and any person appointed by the Court). Defense Counsel shall have access to
23 and may use Protected Material only for the purpose of this action. Prior to receiving
24 access to the Protected Material, Defense Counsel must signify assent to the terms of
25 this Protective Order by executing the acknowledgment attached as Appendix A,
26 indicating that he or she has read and understands this Protective Order and has agreed
27 to be bound by its terms. Defense Counsel shall file the signed acknowledgment with
28 the Court within five (5) calendar days of its execution. Protected Material also may be

1 | disclosed to the following persons:

2 | 1. Defendant. Defendant himself shall not under any
3 | circumstances be permitted to access or view any document, file, or Visual
4 | Depiction containing actual or alleged Child Pornography without petition to, and
5 | further order of, the Court. Defendant may access and review any document, file,
6 | or Visual Depiction that does not contain actual or alleged Child Pornography for
7 | the limited purpose of assisting in the preparation of his defense in the presence of
8 | Defense Counsel and under the direct supervision and control of Defense Counsel.
9 | Prior to receiving access to any Protected Material in accordance with this paragraph,
10 | Defendant must signify assent to the terms of this Protective Order by executing the
11 | acknowledgment attached as Appendix A, indicating that he or she has read and
12 | understands this Protective Order and has agreed to be bound by its terms. Defense
13 | Counsel shall file the signed acknowledgment with the Court within five (5) calendar
14 | days of its execution.

15 | 2. Trial Witnesses. Disclosure may be made to persons
16 | designated as trial witnesses to the extent reasonably necessary in preparing to testify.
17 | Prior to receiving access to the Protected Material, the person to whom disclosure is
18 | made must signify assent to the terms of this Protective Order by executing the
19 | acknowledgment attached as Appendix A, indicating that he or she has read and
20 | understands this Protective Order and has agreed to be bound by its terms. Defense
21 | Counsel shall file the signed acknowledgment with the Court within five (5) calendar
22 | days of its execution.

23 | 3. Outside Consultants and Experts. Disclosure may be made
24 | to one (1) outside consultant or expert retained for the purpose of assisting Defense
25 | Counsel in the defense of this criminal matter to the extent reasonably necessary for the
26 | defense of this criminal matter; provided, however, that the person to whom disclosure
27 | is made must signify assent to the terms of this Protective Order by executing the
28 | acknowledgment attached as Appendix A, indicating that he or she has read and

1 understands this Protective Order and has agreed to be bound by its terms. Defense
2 Counsel shall file the signed acknowledgment with the Court within five (5) calendar
3 days of its execution. If Defense Counsel determines that additional experts are needed
4 to review the material, Defense Counsel must obtain a further order of the Court before
5 allowing any other individual to review the Protected Material.

6 4. Investigator. Disclosure may be made to one (1) investigator
7 retained for the purpose of assisting Defense Counsel in the defense of this criminal
8 matter to the extent reasonably necessary for the defense of this criminal matter;
9 provided, however, that the person to whom disclosure is made must signify assent to
10 the terms of this Protective Order by executing the acknowledgment attached as
11 Appendix A, indicating that he or she has read and understands this Protective Order
12 and has agreed to be bound by its terms. Defense Counsel shall file the signed
13 acknowledgment with the Court within five (5) calendar days of its execution. If
14 Defense Counsel determines that additional investigators are needed to review the
15 material, Defense Counsel shall obtain a further order of the Court before allowing any
16 other individual to review the Protected Material.

17 6. Handling of Protected Material.

18 1. Examination of Protected Material. No person, other than those
19 persons identified in Section 5 who have executed the acknowledgment attached as
20 Appendix A, may examine the Protected Materials without further court order. The
21 Protected Materials must remain under the control of Defense Counsel, and examination
22 of the Protected Materials shall be done in a confined and secure environment which
23 shall be inaccessible to individuals not authorized by the Protective Order. A copy of
24 this Protective Order shall be maintained with the Protected Material at all times. Under
25 no circumstances shall the Protected Materials be mailed, transmitted or otherwise
26 removed from the confined and secure environment.

27 2. Copies of Protected Material. No copies of any document, image
28 file, or Visual Depiction contained in the Protected Materials may be made without

1 further court order. This prohibition includes, but is not limited to, (1) printing out
2 images onto paper or film; and (2) duplicating the images in any digital format.
3 Documents and non-image files such as word processing files, e-mails (redacted of
4 references to Child Pornography, e.g., web-addresses), and other text files may be
5 duplicated to the extent necessary to prepare the defense of this criminal matter. If
6 these documents are printed or duplicated, neither the photocopier nor the printer
7 may be connected to the Internet or any other Computer network. Defense Counsel
8 shall be personally present at all times any Protected Material is duplicated or printed.

9 3. Internet or Network Access. Any Computer from which the
10 Protected Materials will be accessed shall not be connected to the Internet or to any
11 other Computer network.

12 4. Protected Material Filed With Court. Any pleadings that include or
13 make reference to Protected Materials shall be filed under seal. Where reasonably
14 practical, only the portions of documents consisting of Protected Material shall be
15 lodged under seal. No motion or other request to file or lodge Protected Material under
16 seal shall be required. Such Protected Material shall be filed or lodged in sealed
17 envelopes or other appropriate sealed containers. Each sealed envelope or container
18 shall be endorsed with the caption and case number of the action and a statement
19 substantially in the following form:

20 This envelope is sealed pursuant to Order of the Court and contains Protected
21 Material filed in this criminal matter, and is not to be opened or the contents thereof
22 displayed or revealed except by the Court or upon order of the Court.

23 5. Termination of Participation in Action. Once participation in this
24 criminal proceeding by any person obtaining Protected Material pursuant to Section 5
25 has been terminated at the district court level, all Protected Material in the possession of
26 such person shall be returned by such person within ten (10) calendar days to Defense
27 Counsel.

1 6. Final Disposition. Upon final disposition of the above-captioned
2 matter, that is, sentencing by the district court or dismissal of the case, Defense Counsel
3 and the United States shall meet within fifteen (15) calendar days, agree upon, and
4 execute procedures which will result in the non-recoverable destruction of Protected
5 Material, without damage to the Computers, data drives, and components used to
6 examine the Protected Material. The physical Computers, data drives, and components,
7 shall remain the property of Defense Counsel or Defendant's expert, once all Protected
8 Material has permanently been removed by the United States. Unless Defendant is
9 represented by the Federal Public Defender or an attorney appointed pursuant to the
10 Criminal Justice Act, Defendant will bear all costs associated with the destruction of
11 Protected Material.

12 7. Report to Court. Upon final disposition of the above-captioned
13 matter and the destruction of Protected Material as provided for herein, Defense
14 Counsel shall file a brief report with the Court, with a copy to the United States,
15 specifying that the terms of this Protective Order have been complied with and reporting
16 the occurrence of the referenced destruction of Protected Material.

17 7. Amendment. This Protective Order may be amended by agreement of
18 Defense Counsel and the United States in the form of a written stipulation filed with the
19 Court and subject to the Court's approval.

20 8. Effective Period. This Protective Order shall be effective immediately
21 upon entry by the Court. It shall survive termination of this action, and the Court shall
22 retain jurisdiction to enforce or modify its terms.

23 /
24 /
25 /
26 /
27 /
28 /

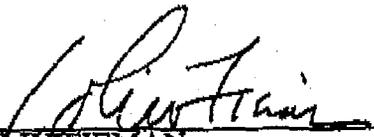
1 9. Penalties for Breach. This Protective Order shall be strictly enforced by
2 the Court, and any violation may result in sanctions by this Court and in state or federal
3 criminal charges for possession or dissemination of Child Pornography.

4
5 IT IS SO STIPULATED.

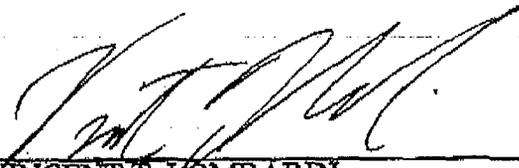
6
7 Dated: 7/8, 2005


Defendant

8
9
10 Dated: 7/8, 2005


COLIN FIEMAN
Attorney for Defendant

11
12
13
14 Dated: 7/9, 2005


VINCENT T. LOMBARDI
Assistant United States Attorney

15
16
17
18 **ORDER**

19 IT IS SO ORDERED.

20
21 Dated: this 21st day of July, 2005.


THE HON. RONALD B. LEIGHTON
UNITED STATES DISTRICT JUDGE

App. C

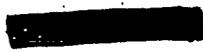
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

SUPERIOR COURT OF WASHINGTON FOR KING COUNTY

STATE OF WASHINGTON,

Plaintiff,

vs.



Defendant,

No. 06-1-06626-6 SEA

STIPULATION AND AGREED
PROTECTIVE ORDER REGARDING
EVIDENCE OF DEPICTIONS OF
CHILDREN ENGAGED IN
SEXUALLY EXPLICIT CONDUCT

This Court, having considered the briefing and arguments of the parties, enters the following order relating to discovery in this matter:

1. The Redmond Police Department is directed to prepare mirror image hard-drives of all computer hard-drives seized from the defendant, pursuant to search warrants, in this matter. The Redmond Police Department shall prepare the above described mirror images within 10 court days from entry of this order.
2. Jan Fuller, of the Redmond Police Department, is directed to personally turn over the mirror image hard drives to the defense expert, Marcus Lawson, of Global CompuSearch, at a mutually agreement time, during business hours, at the Redmond Police Department. Alternatively, Ms. Fuller can provide the same materials to either defense attorney, named below.

STIPULATION AND AGREED PROTECTIVE ORDER - 1

Norm Maleug, Prosecuting Attorney
W554 King County Courthouse
516 Third Avenue
Seattle, Washington 98104
(206) 296-9000
FAX (206) 296-0955

1 Furthermore, this Court enters the following protective order relating to the mirror image hard
2 drives referenced above. This Protective Order applies to defense counsel, John Henry Browne
3 and Jessica Riley, their agents and employees, as well as to their endorsed expert, Marcus
4 Lawson and his agents and employees.
5

6 3. Prior to being provided with the mirror image hard drives referenced herein,
7 defense counsel shall serve Mr. Lawson, as well as his agents and employees
8 (Josiah Roloff, Kevin Peden and/ Carol Peden) with a copy of this order, and Mr.
9 Lawson, Josiah Roloff, Kevin Peden and Carol Peden must sign the order, and the
original signed order must be filed with the court. Mr. Browne and Ms. Riley are
also required to sign this order.

10 4. Once he takes possession of the mirror image hard-drives, Mr. Lawson and his
11 agents and employees (Josiah Roloff, Kevin Peden and Carol Peden) shall
12 maintain exclusive custody of the mirror-image hard-drives. Mr. Lawson and his
13 agents and employees shall be the sole defense experts maintaining control of,
14 and access to, these hard-drives. Mr. Lawson, Josiah Roloff, Kevin Peden and
15 Carol Peden, shall not share the contents of the mirror image hard drives with any
other person, including any agents or employees. Mr. Lawson, Josiah Roloff,
Kevin Peden and Carol Peden, when not actually performing analysis on the hard
drives, shall maintain the same in a location which is secure, and not subject the
mirror image hard drives to unauthorized duplication or theft.

16 5. Mr. Lawson, Josiah Roloff, Kevin Peden, and Carol Peden shall not share or
17 disclose the results of their work with any person other than the defendant's
18 attorneys, John Henry Browne and Jessica Riley.

19 6. Neither Mr. Lawson, Josiah Roloff, Kevin Peden and Carol Peden, nor defense
20 counsel, may provide the defendant with his own copy of Mr. Lawson's work
21 product, or any other information found on the hard drives examined by Mr.
22 Lawson. This provision does not preclude defense counsel or Mr. Lawson, Josiah
23 Roloff, Kevin Peden and Carol Peden, from reviewing the results of Mr. Lawson's
analysis with the defendant, but neither Mr. Lawson, Josiah Roloff, Kevin Peden
and Carol Peden nor defense counsel may share, disclose, or reveal to the
defendant any photographs or other digital images recovered by Mr. Lawson,
prior the defense seeking and obtaining a specific order from the court allowing
these materials to be shared with the defendant, upon a showing that is necessary

STIPULATION AND AGREED PROTECTIVE
ORDER - 2

Norm Maleng, Prosecuting Attorney
W554 King County Courthouse
516 Third Avenue
Seattle, Washington 98104
(206) 296-9000
FAX (206) 296-0055

1 for the defendant to view specific photographs or other digital images located by
2 Mr. Lawson.

3 7. At the conclusion of his testimony, or the conclusion of trial in this matter,
4 whichever comes earlier, Mr. Lawson, Josiah Roloff, Kevin Peden and Carol
5 Peden shall:

6 A. Personally return the mirror image hard-drives to a representative of the
7 Redmond Police Department, either at the Redmond Police Department or
8 at the King County Superior Court, provided a representative of the
9 Redmond Police Department is available at the conclusion of Mr.
10 Lawson's testimony;

11 B. Within three days of his testimony being completed, destroy any work
12 product, including any photographs or other digital images produced from
13 the hard-drives, and any and all digitally maintained photographs taken
14 from the hard drives;

15 8. At the conclusion of trial defense counsel shall destroy all photographs produced
16 from the hard-drives produced by the Redmond Police Department, and destroy
17 any and all digitally maintained photographs taken from these hard drives. In the
18 event defense counsel wishes to preserve any of these items for purposes of
19 appellate review, if any, defense counsel shall seek a specific order from the court
20 which allows defense counsel to file the same, under seal, with the court.

21 9. Provided that defense counsel seeks to use any photographs, whether actual or
22 digital, defense counsel shall file the same with the court under seal. Under no
23 circumstances shall defense counsel attach photographs, obtained by Mr. Lawson,
24 Josiah Roloff, Kevin Peden and Carol Peden, to their pleadings, which would be
25 subject to public inspection.

26 10. Materials provided to defense counsel, by Mr. Lawson, Josiah Roloff, Kevin
27 Peden and Carol Peden, shall remain in the exclusive custody of defense counsel
28 and not be shown to their agents and employees. Any reproduction of these
29 materials, in preparation for trial, shall be performed solely by defense counsel.
30 When not actually reviewing materials produced by Mr. Lawson, Josiah Roloff,
31 Kevin Peden and Carol Peden, defense counsel shall maintain the same in a
32 location which is secure, and not subject to unauthorized duplication or theft.

33 11. The hard drives, as well as any reports of photographs Mr. Lawson and his agents
and employees produces from the hard drives, shall not be used for any purpose
other than to prepare for the defense of the named defendant in the above-entitled
cause.

STIPULATION AND AGREED PROTECTIVE
ORDER - 3

Norm Maleng, Prosecuting Attorney
2551 King County Courthouse
316 Third Avenue
Seattle, Washington 98104
(206) 296-4000
FAX (206) 296-0959

12. The hard drives, as well as any reports of photographs Mr. Lawson, and his agents and employees produces from the hard drives shall not be given, loaned, sold or shown to any member or associate of the media unless expressly permitted by court order.

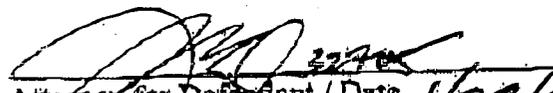
13. The hard drives, as well as any reports of photographs Mr. Lawson, as well as his agents and employees produces from the hard drives shall not be publicly exhibited, shown, displayed or used in any fashion except judicial proceedings in the above entitled cause, and as described herein.

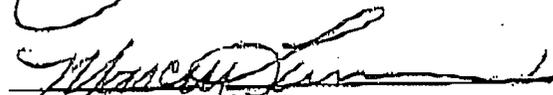
14. Violation of this order is subject to sanctions by the court.

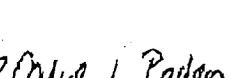

Catherine Sheaffer / Judge


Deputy Prosecuting Attorney / Date


Attorney for Defendant / Date 1-29-07


Attorney for Defendant / Date 1/29/07


Marcus Lawson / Date 1/26/07

 Date  Date 1/27/2007  Carol Peden

STIPULATION AND AGREED PROTECTIVE ORDER - 4

Norm Malong, Prosecuting Attorney
W354 King County Courthouse
516 Third Avenue
Seattle, Washington 98104
(206) 296-9000
FAX (206) 296-0055

App. D

WA COHEN

FILED
SUPERIOR COURT
THURSTON COUNTY WASH

Honorable Richard A. Strophy

'03 APR -7 AM 11:21

RETT: J. DOUGL CLERK

BY _____ DEPUTY

THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THURSTON COUNTY

STATE OF WASHINGTON,

Plaintiff,

v.

[REDACTED]

Defendant.

CAUSE NO. 02-1-0960-7

**STIPULATION AND AGREED
PROTECTIVE ORDER REGARDING
EVIDENCE OF ALLEGED DEPICTIONS
OF CHILDREN ENGAGED IN
SEXUALLY EXPLICIT CONDUCT**

The defendant, [REDACTED], and the Thurston County Prosecuting Attorney, by and through their respective counsel, hereby stipulate to the entry of a protective order regarding visual material evidence of the alleged crime of dealing in or possession of depictions of minors engaged in sexually explicit conduct - including without limitation photographs, videotapes and computer-generated images - provided in the course of discovery in the above-entitled cause and agree to the following conditions which apply to defense counsel, their employees and agents therefore,

IT IS HEREBY ORDERED:

1. That the State shall provide defendant's counsel with a mirrored copy of the hard drive seized in this case and a copy of any disks seized, necessarily including any and all alleged child pornography and/or contraband allegedly contained thereon;

2. That in connection with the provision of such copies, defense counsel will furnish the State with hard drives and/or other necessary computer media onto which the mirror image copies will be replicated so that they function as readily as the original;

STIPULATION AND AGREED PROTECTIVE
ORDER REGARDING EVIDENCE . . . - Page 1

COHEN & IARIA
Hillclimb Court, Suite 108
1425 Western Avenue
Seattle, Washington 98101
206-624-9694

1 3. That the mirror image copy referenced above and any disks shall be maintained by
2 defense counsel and/or an expert retained by the defense in accordance with the terms of this
3 order and shall be used by counsel and/or the expert solely and exclusively in connection with
4 this case (including trial preparation, trial, and appeals or other related legal proceedings) and
5 for no other purposes;

6 4. That the data contained on the mirrored drive and disks may be accessed and
7 viewed only by defense counsel, the defense expert, and defense investigators;

8 5. That defense counsel or the defense investigator shall deliver the drive and disks
9 to the defense expert via Federal Express;

10 6. That the data shall be password protected. The password shall be maintained by
11 law enforcement and shall not be released other than directly to undersigned defense counsel
12 and/or to the defense expert. Defense counsel and/or the defense expert shall not further
13 distribute the password;

14 7. That the computer into which the mirrored drive and any disks may be inserted for
15 access and operation shall not be connected to a network or modem while the mirrored drive
16 is installed, or at any time prior to the destruction of all data as specified in paragraph 11;

17 8. That the computer into which the mirrored drive or disks are inserted may be
18 connected to a printer only on the following terms and conditions – that any printer utilized is
19 a local printer, that such printer may be connected only when and as necessary to print
20 non-graphic image files (text files, log files, directory trees, etc.), and that defense counsel, the
21 defense expert or a defense investigator shall be personally present at all times a printer is
22 connected;

23 9. That in no event shall any graphic image file containing child pornography or
24 which may reasonably be construed as constituting child pornography be copied, duplicated or
25 replicated, in whole or in part, onto any external media including, but not limited to, paper,
26 floppy disk, CD-ROM, DAT tape, zip disk, or other media;

27 ///

28 ///

1 10. That the mirrored drive and disk(s) shall be maintained by defense counsel and/or
2 the defense expert in a locked file or cabinet at all times except when being transported and/or
3 actively utilized as provided for herein;

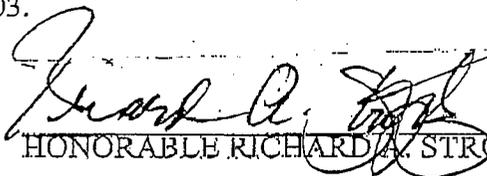
4 11. That a copy of this order shall be kept with the mirrored drive and disk(s) at all
5 times;

6 12. That upon termination of this matter, the defense shall arrange for the destruction
7 of the hard drive;

8 13. That upon termination of this matter and destruction of the hard drive, defense
9 counsel shall file a brief report with the Court, with a copy to government counsel, specifying
10 that the terms of this Order have been complied with and reporting the occurrence of the hard
11 drive destruction;

12 15. That defense counsel shall be permitted reasonable access to defendant's original
13 computer system for viewing and visual inspection.

14 DATED this 7th day of April, 2003.


HONORABLE RICHARD A. STROPHY

17 Presented by:

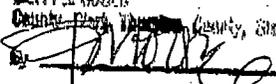
18 
19 Jeffrey D. Cohen
20 WSBA #11085

21 Approved by:

22 
23 Christen Lee Anton Peters
24 WSBA #23559

25 STATE OF WASHINGTON
26 County of Thurston
I, Betty J. Gould, County Clerk and Ex-Officio Clerk of the
Superior Court of the State of Washington, for Thurston County
holding record of three do hereby certify that the foregoing
is a true and correct copy of the original and same appears on
file and of record in my office under No. three pages.
IN WITNESS WHEREOF, I have hereunto set my hand and
affixed the seal of said court, this

27 7th day of April, 2003

28 BETTY J. GOULD
County Clerk, Thurston County, State of Washington

Deputy

App. E

1 3. That the bit by bit or mirror image copies referenced (hereinafter the "Mirrored
2 Drives") shall be maintained by defense counsel and/or an expert retained by the defense in
3 accordance herewith, including Marcus Lawson of Global CompuSearch, and shall be used
4 by counsel and/or the expert solely and exclusively in connection with this case (including
5 trial preparation, trial and appeals or other related legal proceedings) and for no other
6 purposes;
7

8 4. That the data contained on the Mirrored Drives may be accessed and viewed
9 only by defense counsel, the defense expert, and defense investigators;
10

11 5. That defendant himself shall not under any circumstances be permitted to access
12 or view any graphic image file containing actual or alleged child pornography without petition
13 to and further order of the Court; however, defendant may access and view non-image data
14 on the Mirrored Drives for the purpose of assisting in the preparation of his defense in the
15 presence of counsel and under the direct supervision and control of counsel;
16

17 6. That the computer into which the Mirrored Drives may be inserted for access
18 and operation shall not be connected to a network while the Mirrored Drives are installed; or
19 at any time prior to destruction of all data as specified in Paragraph 10;
20

21 7. That the computer into which the Mirrored Drives are inserted may be
22 connected to a printer only on the following terms and conditions - that any printer utilized
23 is a local printer, that such printer may be connected only when and as necessary to print non-
24

25
26
27 DISCOVERY ORDER -- 2
ado37

1 graphic image files (text files, log files, directory trees, etc.), and that defense counsel or a
2 defense investigator shall be personally present at all times a printer is connected;

3 8. That the Mirrored Drives shall be maintained by defense counsel and/or the
4 defense expert in a locked file or cabinet at all times except when being actively utilized as
5 provided for herein;

7 9. That a copy of this Order shall be kept with the Mirrored Drives at all times;

8 10. That upon termination of this matter the parties shall meet, agree upon, an
9 execute procedures which will result in the non-recoverable destruction, without damage to
10 the hardware, of all data on the Mirrored Drives, and all computers and computer components
11 used to examine such data. The physical hard drives, computers, and computer components,
12 once the data have been removed, shall remain property of defense counsel or the defense
13 expert;

14 11. That any dispute as to appropriate data destruction procedure will be resolved
15 by the Court;

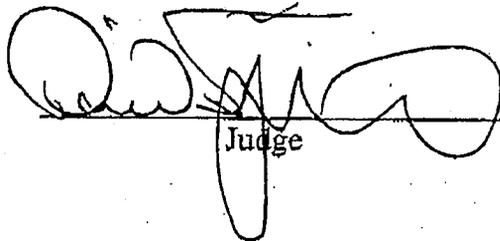
16 12. That upon termination of this matter and data destruction as provided for herein,
17 defense counsel shall file a brief report with the Court, with a copy to Plaintiff's counsel,
18 specifying that the terms of this Order have been complied with and reporting the occurrence
19 of the referenced data destruction;

20 13. That defense counsel shall be permitted reasonable access to Defendant's
21 original computer system for viewing and visual inspection.
22
23

24
25
26
27 DISCOVERY ORDER -- 3
ado37

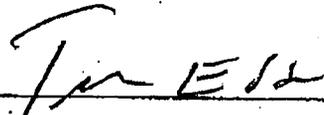
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

DATED: This 21st day of MARCH, 2003.



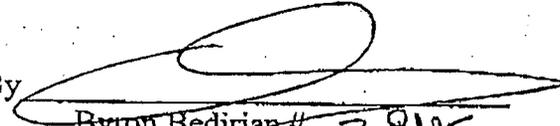
Judge

Presented by:
Nuxoll, Libey, Ensley, Esser & Nelson
Attorneys for Defendant

By 

Timothy Esser #6864

Whitman County Prosecutor's Office
Attorneys for Plaintiff

By 
Byron Bedirian # 29195
Sr. Deputy Prosecutor

DISCOVERY ORDER -- 4
ado37

NUXOLL, LIBEY, ENSLEY, ESSER & NELSON
ATTORNEYS AT LAW
520 EAST MAIN
PULLMAN, WASHINGTON 99163
(509) 332-7682 FAX (509) 334-2205

App. F

Received & Filed
LEWIS COUNTY, WASH
Superior Court

FEB 22 2002

By: Nettle Jungers, Clerk *NW*
Deputy

IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF LEWIS

11	State of Washington)	
12)	
13	v.)	Case No.: 01-1-697-0
14	William [REDACTED])	AGREED
15)	ORDER FOR DISCOVERY
16)	

THIS MATTER coming before the Court of Defendant's Motion for Discovery under CrR 4.7,
and the Court having considered the entirety of the records and files herein, and good cause appearing
therefore,

IT IS HEREBY ORDERED:

1. That the State shall provide defendant's counsel with two (2) bit by bit (also known as mirror image) copies of hard drives from all computers seized in this case, necessarily including any and all child pornography and/or contraband allegedly contained thereon;
2. That the mirror image copies will be replicated so that they functions as readily as the original;
3. That the bit by bit or mirror image copies referenced above (hereinafter the "Mirrored Drives") shall be maintained by defense counsel and/or an expert retained by the defense in accordance

BACKLUND & MISTRY
Attorneys at Law

331 NW Park Street
Chehalis, WA 98532
(360) 740-4445
FAX: 740-1650

attys

1
2
3 herewith and shall be used by counsel and/or the expert solely and exclusively on connection
4 with this case (including trial preparation, trial and appeals or other related legal proceedings)
5 and for no other purposes;

- 6 4. That the data contained on the Mirrored Drive may be accessed and viewed only by defense
7 counsel, the defense expert, and defense investigators;
- 8 5. That defendant himself shall not under any circumstance be permitted to access or view any
9 graphic image file containing actual or alleged child pornography without petition to and
10 further order of the Court;
- 11 6. That the computer into which the mirrored Drive may be inserted for access and operation shall
12 not be connected to a network while the Mirrored Drives are installed, or at any time prior to
13 the destruction of all data as specified in paragraph 11;
- 14 7. That the computer into which the mirrored Drive are inserted may be connected to a printer
15 only on the following terms and conditions – that any printer utilized is a local printer, that
16 such printers may be connected only when and as necessary to print non-graphic images files
17 (text files, log files, directory trees, ect.), and that defense counsel or a defense investigator or
18 the expert shall be personally presents at all times a printer is connected;
- 19 8. That in no event shall any graphic image file containing child pornography or which may
20 reasonably be construed as constituting child pornography be copied, duplicated or replicated,
21 in whole or in part, onto any external media including, but not limited to, paper, floppy disk,
22 CD-ROM, DAT tape, zip disk, or other media;
- 23 9. That the mirrored Drive shall be maintained by defense counsel and/or the defense expert in a
24 locked file of cabinet at all times except when being actively utilized as provided for herein;
- 25 10. That a copy of this Order shall be kept with the Mirrored Drives at all times;
- 26 11. That upon termination of this matter the parties shall meet, agree upon, and execute procedures
27 which will result in the non-recoverable destruction, without damage to the hardware, of all
28
29
30

BACKLUND & MISTRY
Attorneys at Law

331 NW Park Street
Chchalis, WA 98532
(360) 740-4445
FAX: 740-1650

1
2
3 data on the Mirrored Drives, and on all computers and computer components used to examine
4 such data. The computers, and computer components, once the data have been removed, shall
5 remain property of the defense expert; the hard drive shall be returned to the State.

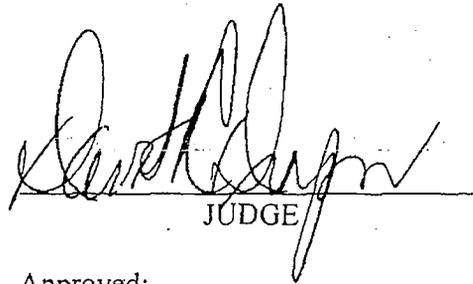
6 12. That any dispute as to appropriate data destruction procedure will be resolved by the Court;

7 13. That upon termination of this matter and data destruction as provided for herein, defense
8 counsel shall file a brief report with the Court, with a copy to the government counsel,
9 specifying that the terms of this Order have been complied with and reporting the occurrence
10 of the referenced data destruction;

11 14. That defense counsel shall be permitted reasonable access to the original computer system for
12 viewing and visual inspection.

13 15. All of the above are contingent on technical feasibility.

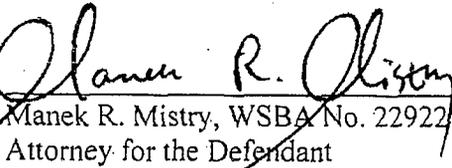
14 DONE this 22 day of ^{February} ~~January~~, 2002

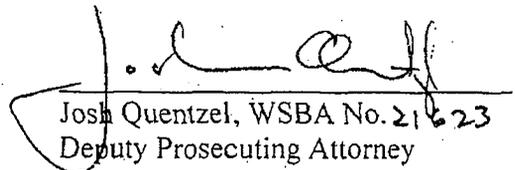
15
16
17 
18 JUDGE

19 Presented by:

Approved:

20 **BACKLUND & MISTRY**

21 
22 Manek R. Mistry, WSBA No. 22922
23 Attorney for the Defendant

24
25
26 
27 Josh Quentzel, WSBA No. 21623
28 Deputy Prosecuting Attorney

29 **BACKLUND & MISTRY**
30 Attorneys at Law

331 NW Park Street
Chehalis, WA 98532
(360) 740-4445
FAX: 740-1650