Legislative Testimony

Oregon Criminal Defense Lawyers Association

April 1, 2013

The Honorable Floyd Prozanski, Chair
The Honorable Betsy Close, Vice-Chair
Senate Judiciary Committee, Members

RE: Senate Bill 409

Dear Chair Prozanski and Members,

The Oregon Criminal Defense Lawyers Association is an organization of attorneys who represent juveniles and adults in delinquency, dependency, and criminal prosecutions and appeals throughout the state of Oregon. Thank you for the opportunity to submit the following comments in support of Senate Bill 409.

What is at issue in SB 409: SB 409 addresses the need for enhanced protections in the pretrial discovery phase of handling evidence that "*constitutes or contains a visual depiction or audio recording involving a child in a state of nudity or engaged in sexually explicit conduct.*"

Of late, the state has been requesting court orders forbidding the production of copies of such materials to the defense in the normal course of discovery, but rather requiring the defense to examine the evidence in the police evidence custodian facility.[1] SB 409 resolves this dispute by adopting the method employed by the State of Washington, which mandates pretrial production of the evidence to both the defense and the prosecution under the same terms of a wrap-around protective order. The protective order must:

- restrict use of the material for any purpose unrelated to the criminal case;
- require the property be kept "*secure against theft and inadvertent disclosure and in a manner that deters copying or dissemination*;"
- prohibit disclosure except to the defense attorney or prosecuting attorney, and their experts as necessary for case preparation;
- require that the defense attorney and prosecuting attorney assure the expert receives and signs a copy of the protective order and complies with its terms;

[1] Proponents of this method of forbidding production of the materials to the defense have introduced HB 3048 on the House side. HB 3048 received a public hearing on Monday April 1 before the HJUC.

- prohibits the defendant from viewing or examining the property outside the presence of the defense attorney;
- require return of all such property and executed copies of the protective order at the conclusion of the case, with certification by the attorneys and experts that no part of the property or material has been retained.

How SB 409 changes existing law: It is completely appropriate that evidence of a highly sensitive nature, particularly involving a minor, be treated with the utmost care and confidentiality. The customary practice has been for the state to provide copies of all sorts of sensitive materials to the defense under the terms of a carefully constructed protective order. Current ORS 135.873 (2) empowers the court to "*deny, restrict or defer*" the production of discovery, or to "*make such other order as is appropriate.*" Specifically with respect to a "*sexual offense, an offense involving the visual or audio recording of sexual conduct by a child or invasion of personal privacy*," ORS 135.873 (6) requires the court to issue a protective order if requested by the district attorney.

As mentioned, the state has begun to request court orders precluding production of copies for the defense, and instead making the evidence available for examination in a law enforcement facility. SB 409 is more closely aligned with customary practice by *mandating* a protective order in all cases where evidence is of this nature. Further, SB 409 delineates the terms which the mandatory protective order must contain.

To what type of evidence does SB 409 apply? The type of evidence to which SB 409 applies is quite broad. Many different kinds of criminal cases involve evidence that "*constitutes or contains a visual depiction or audio recording involving a child in a state of nudity or engaged in sexually explicit conduct.*" SB 409 is *not* confined to child pornography or evidence which of itself is criminal to possess.

Examples of the types of evidence to which SB 409 applies are:

- Photographs of intimate body parts taking by medical professionals in the course of a child-abuse medical evaluation in a child abuse investigation;
- Images voluntarily taken by a minor in a state of nudity and sent by text message to another (i.e., "sexting);
- Visual images of nakedness or sexual activity displayed on Facebook or other social media;
- Images of digitally-altered photographs that are simulated to appear to be children, but are not;
- Images of child pornography, criminal in their possession.

Why SB 409 is necessary: As mentioned, the counties are resolving this dispute of handling this sensitive evidence on a case-by-case basis, with inconsistent results. Some courts are requiring production of the material under a protective order; other courts are requiring the defense to access the evidence at the law enforcement facility.

The issue of equal access to the evidence is of critical importance to the defense. In most criminal cases involving child sexual activity, both the state and the defense consult with experts for purposes of case preparation. Examples:

- Forensic photographs are often taken during a medical examination of a child's vaginal or rectal area; these photographs may, or may not, indicate tears or irregularities that are, or are not, consistent with the allegations of abuse. Both the prosecution and the defense consult with and rely upon the opinions of experts to review these photographs to develop their theory of the case or defense. Most often, these expert witnesses reside in the metropolitan area; sometimes they reside out-of-state. It is doubtful that most experts would be willing to consult with defense counsel if they must travel to far-reaching corners of Oregon before examining the images.

- With respect to electronic media crimes (i.e., visual images on a computer), consultation with a forensic computer examiner and/or a digital imaging expert is necessary. An expert can detect a host of issues: when an image was downloaded; how it was downloaded; whether the user affirmatively searched for the image or whether a virus populated the image; whether files are password protected; whether the computer has multiple user accounts; whether imagery is digitally altered, comes from an internet site, or was uploaded from a camera.

With respect to forensic computer experts, undertaking this search query can take hours, often days, and requires the use of specialized equipment that the expert must import. It is for this very reason that search warrants are issued for the *seizure* of computers so the law enforcement forensic computer examiners can review the computer under the accommodations of their laboratory, rather than be forced to conduct the examination at the sight of the residence. Toward that end, I attach to my written comments a search warrant affidavit submitted by Sergeant Joshua S. Moulin with the Central Point Police Department attesting to this very need.

In confining the forensic computer examination to a government facility, it is not uncommon for defense experts to experience the following:

- Difficulty scheduling time with the law enforcement evidence custodian. Typically, the evidence custodian confines access to business hours and/or when staff is available. It is not uncommon that the first appointment is delayed a matter of weeks from the initial request. If the defense expert needs more time than initially anticipated, the expert must go to the end of the queue and request a future appointment at a later date.

- Insufficient room and accommodations in which to place their own equipment, manuals, etc.

- A lack of productivity while the computer programs run their course, often for many hours extended over several days. The hours spent by the expert waiting for the program to run are chargeable to the defense.

- The ability of law enforcement's forensic computer experts to recreate and discern what search queries the defense expert undertook.

- Insufficient accommodations for private consultations with defense attorney alone, or with the defendant.

The defense attorney experiences the following limitations:

- The defense must disclose to the state at an early stage the fact that it is consulting with an expert, and the identity and type of expert. Any experienced litigator (civil or criminal) will acknowledge that *if* they are consulting with an expert, *who* that expert is, *what* they are consulting with that expert about, and *how much time* they spend consulting together are all instances of work-product privacy customarily afforded to parties in litigation.

- For a client in custody (and many facing these sort of charges are), it is difficult, expensive, and sometimes impossible to discuss the results of the search query with the client. In order to consult with the defendant in the presence of the evidence, jail staff would need to transport the accused under guard, and even then, the degree of confidential communication can be compromised.

- Access to documents and records immediately prior to trial, and during trial, are critical for any trial lawyer. Documents take on new meaning and significance

  as evidence unfolds during the course of testimony. Being deprived of immediate and confidential access to the documents can seriously impede the ability to respond to the flow of testimony.

SB 409 avoids costly litigation: Opponents of SB 409 may claim that restricting defense access to this evidence is mandated by the Adam Walsh Child Protection and Safety Act, 18 USC §3509 (m). The case law is fairly resolved, however, that the Adam Walsh Act applies to federal prosecutions and does not preempt state laws. *See State v. Norris,* 236 P.3d 225 (Wash. 2010).

An unintended consequence of the Adam Walsh provision in federal court is increased pre-trial litigation challenging the adequacy and reasonableness of the access and accommodations afforded the defense. While it is true that the Adam Walsh provision has

survived constitutional challenges *on its face*, it is the subject of constant pre-trial litigation on a *case-by-case* basis. *See, e.g., US v. Knellinger,* 471 F. Supp. 2d 64 (E.D. Va. 2007); *US v. Winslow,* 2008 U.S. Dist. LEXIS 66855 (D. Alaska 2008); *US v. Bortnick,* 2010 WL 935842 (D. Kan. 2010).

Allowing both parties equal access to the materials under a mandatory protective order is balanced, fair and efficient. SB 409 is consistent with the practice adopted by the Washington Supreme Court. In *State v. Boyd,* 160 Wn. 2d 424, 158 P3d 54, 62 (2007), it stated:

> *In cases such as these, safeguarding the interests of the victims requires conditions that account for the ease with which the evidence can be disseminated. The defendant should be allowed access to the evidence only under defense counsel's supervision. Defense counsel is personally and professionally responsible for any "unauthorized" distribution of or access to the evidence. Access by non-counsel must be preceded by court order. The evidence must be secured and inaccessible to anyone besides defense counsel. The evidence must be promptly returned at the end of the criminal proceeding. Access may only be for purposes of the action. Any order should also prohibit the making of additional copies, require that a copy of the order be kept with the evidence, bar its digitization, and obligate the defense to pay the reasonable cost of duplication. It is also appropriate to require a firewall between the Internet and any computer used to access the protected materials during its inspection, to return the evidence if representation is terminated, and to clear any computer used in the examination of this evidence of its traces before that computer is accessible for other purposes.*

Enforcement powers of the court and the Oregon State Bar: Violation of the terms of the mandatory protective order will be enforceable by the court under its powers of contempt. [ORS 33.015 *et seq.*] Additionally, the defense attorney and district attorney will be subject to the disciplinary sanctions of the Oregon State Bar, which includes suspension or disbarment. [See paper under title "House Bill 2344: Response to questions regarding implications of violating a protective order under Oregon State Bar disciplinary rules."]

For all these reasons, OCDLA urges the Committee to pass SB 409

Thank you for your consideration of these comments. Please do not hesitate to contact me if you have any questions.

Respectfully submitted,

Gail L. Meyer, JD
Legislative Representative
Oregon Criminal Defense Lawyers Association
glmlobby@nwlink.com

IN THE CIRCUIT COURT OF THE STATE OF OREGON

FOR THE COUNTY OF JACKSON

STATE OF OREGON)
) SS. AFFIDAVIT FOR SEARCH WARRANT
COUNTY OF JACKSON)

I, Joshua S. Moulin, being first sworn on oath do hereby depose and say:

That I am a Sergeant with the City of Central Point Police Department, located in the County of Jackson, State of Oregon and have been a Police Officer since June 18th 2001. During my tenure as a Police Officer I have worked for both the Ashland Police Department and the Central Point Police Department. I have worked as a Patrol Officer, Field Training Officer, Officer-in-Charge, Arson Investigator, Detective, Forensic Computer Examiner and Sergeant. I have experience with the preparation and execution of search warrants for a variety of crimes. I obtained my Associates of Science Degree from Rogue Community College in 2001, majoring in Fire Science.

I am currently assigned as the Technical Services Bureau Sergeant and Southern Oregon High-Tech Crimes Task Force Commander. As a Sergeant and Forensic Computer Examiner my duties include the investigation of all crimes involving technology and all major crimes. I routinely examine various types of electronic storage media, including hard drives for evidence of criminal wrongdoing. As part of my duties, I examine items such as computer hard drives, storage devices, cellular phones, personal data assistants, and other high-tech devices.

I currently hold an Intermediate Certificate from the Department of Public Safety Standards and Training and have had hundreds of hours in law enforcement training in various topics. I am one of approximately 600 Certified Forensic Computer Examiners (CFCE) and Certified Electronic Evidence Collection Specialists (CEECS) in the world. I have been trained in computer forensics by organizations such as the International Association of Computer Investigative Specialists (IACIS), The Internet Crimes Against Children (ICAC), The National White Collar Crime Center (NW3C), AccessData Corporation, the National Center for Missing and Exploited Children (NCMEC), SEARCH, and the United States Army. I have been qualified as an expert witness in the area of digital evidence forensics. I have been trained in the proper search and seizure of digital evidence, forensic imaging techniques, forensic examinations of digital evidence, courtroom testimony, expert witness testimony, undercover Internet stings and operations, chat rooms, computer hardware and software, cellular telephone communications, identification of child pornography and many

drivers, as well as any application software which may have been used to create the data whether stored on hard drives or external memory storage devices.

I know through my training and experience that it is common for law enforcement to seize all computer items (hardware, software and related instructional material) to be processed at a later date by a qualified computer forensic expert in a laboratory or other controlled environment. This is almost always true because of the following:

a) Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b) Searching computer systems requires the use of precise scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. This requires searching authorities to examine all of the stored data to determine whether it is included in the warrant. This sorting process can take weeks or months depending on the volume of data stored and it would be impractical to attempt this kind of search on sight at the time that the warrant is executed. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c) The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 100 gigabytes of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 7.5 million