

RECORD IMPOUNDED

NOT FOR PUBLICATION WITHOUT THE
APPROVAL OF THE APPELLATE DIVISION

SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-4543-07T4

STATE OF NEW JERSEY,

Plaintiff-Appellant,

v.

ROSS FINESMITH,

Defendant-Respondent.

APPROVED FOR PUBLICATION

July 13, 2009

APPELLATE DIVISION

Submitted October 28, 2008 - Decided July 13, 2009

Before Judges Skillman, Collester and Grall.

On appeal from the Superior Court of
New Jersey, Law Division, Somerset County,
Indictment No. 05-07-111-S

Anne Milgram, Attorney General, attorney for
appellant (Kenneth R. Sharpe, Deputy Attorney
General, of counsel and on the brief).

Fox Rothschild and Brickfield and Donohue,
attorneys for respondent (Alain Leibman and
Paul B. Brickfield, on the joint brief).

The opinion of the court was delivered by

COLLESTER, J.A.D.

Pursuant to leave granted, the State appeals from that
portion of the March 3, 2008 order limiting the temporal scope
of a communications data warrant (CDW) issued pursuant to

N.J.S.A. 2A:156A-29(c) and (e) to a two-week period. We reverse.

In October 2004, the New Jersey State Police Digital Technology Investigation Unit received information from the Wyoming Internet Crimes Against Children Task Force that certain Internet Protocol (IP) addresses assigned to New Jersey residents were making or had been making available pornographic videos and images involving children to others through peer-to-peer filing networks accessed through downloading and installing a file sharing program.¹ As the possession, receipt, and distribution of child pornography is prohibited by N.J.S.A. 2C:24-4b(5)(a) and (b), State Grand Jury subpoenas were issued to Internet Service Providers (ISPs) for subscriber information on the IP addresses. Optimum Online responded to the subpoena by disclosing that one IP address was in the name of Leslie Finesmith in Basking Ridge. Further investigation by the State Police disclosed that Leslie Finesmith is the wife of defendant, Dr. Ross Finesmith, a medical doctor and pediatric neurologist, who lives at the Basking Ridge address with his wife and three daughters, ages eleven, fourteen, and fifteen.

¹ By installing peer-to-peer technology, an individual user is connected to all users of that peer-to-peer software without need for a centralized server in such a network. See generally, Clifford S. Fishman and Anne T. McKenna, Wiretapping and Eavesdropping, § 21.3, pp. 21 (West 3d ed. 2007).

On January 27, 2005, the State Police executed a search warrant on the Basking Ridge residence. Six computers and related media were seized: two desktop computers in the daughters' upstairs bedrooms, two on the first floor, one in an area of the basement used as a home office, and a laptop found in defendant's Honda minivan parked in the garage.² Forensic analysis of the desktop computer in the home office identified child pornography offered in the same manner as the child pornography found by Wyoming authorities. Subsequent analysis of the laptop computer also revealed the presence of child pornography that was last viewed the day before the date of execution of the search warrant.

Defendant was arrested on the date the warrant was executed. On July 14, 2005, he was indicted by the State Grand Jury on charges of second-degree endangering the welfare of a child by distribution of child pornography, in violation of N.J.S.A. 2C:24-4(b)(5)(a) (count one), and fourth-degree endangering the welfare of a child (possession of child pornography), in violation of N.J.S.A. 2C:24-4(b)(5)(b) (count two).

² In a separate opinion, we have upheld the denial of defendant's motion to suppress evidence of the laptop and its contents. State v. Finesmith, 406 N.J. Super. 510 (App. Div. 2009).

The central issue in controversy is the identity of the person who downloaded the child pornography on to the home office desktop computer and the laptop computer. The defense strongly contests that defendant was the "offeror" and possessor of the child pornography and has suggested another member of the household was responsible. To rebut any such defense, the State made an ex parte application to the trial judge³ for a CDW to require an ISP called "DocISP," a provider of email services for doctors, to provide electronic communications of the defendant as a registered user including:

Emails with attachments, opened or unopened; subscriber name, address, contact numbers; all associated information including but not limited to billing information; method and history of payment; usage; access; internet protocol logs; customer service records; static or dynamic protocol address; and any information located on the DocISP service or other databases that indicate internet sites, chat rooms or any activity or service provided by or through DocISP to its associated user Ross Finesmith.

The application sought the stored electronic content without a limitation as to the temporal scope. The State subsequently advised the court that the available stored electronic content for DocISP included electronic mail received

³ The trial judge was and is designated to receive applications and enter orders authorizing interceptions of electronic communications under N.J.S.A. 2A:156A-8.

and undeleted by the user for the period of June 28, 2004 to January 28, 2005.

The affidavit of Detective Sergeant Gorman in support of the CDW stated that on January 23, 2005, the person using the laptop accessed defendant's DocISP email account, read at least six messages, and deleted 123. The user also visited three medical sites and attempted to read a news article titled "Pediatric Patients Get Poor Follow-Up After ADHA Diagnosis," on one of the sites. About thirty minutes later, during the same computer session, the user downloaded a peer-to-peer internet file sharing program and used it to download files named with child pornography keywords.

The trial judge declined to consider the State's CDW application on an ex parte basis, requiring instead that the State present the application as a motion with notice to defendant. At oral argument the Deputy Attorney General argued that the State sought the stored electronic content in the DocISP account for an extended period to show defendant's regular use of the account and prove by circumstantial evidence that he downloaded child pornography on January 23, 2005. While the State contended it was entitled to all stored electronic content on DocISP for its investigation, it agreed to limit its

CDW application to the one-year period from June 28, 2004 to the January 27, 2005, date of the execution of the search warrant.

The judge found that the State made a sufficient showing for issuance of the CDW, but limited the timeframe to the two-week period before the date of the execution of the search warrant:

Frankly, the State has met the burden of showing that material may be relevant to facts in this case. The investigation is ongoing in the respect that the case is still open. The case has not been resolved, so it's an ongoing investigation.

There has been in the course of this case an attempt to indicate that others in the household were using the computer, and so information as to who actually was on the site that day would be quite relevant.

In reviewing the affidavit supplied by the detective, it seems that less than 30 minutes prior to downloading of the installing of the Shareaza peer-to-peer file which led to the downloading of the child pornography matters that the person on the computer was using doc ISP and plugging into medically – medical-type of information that is probable that only a medical physician would tie into. Also, there's information in the case that particularly the laptop is used apparently exclusively by the defendant, Dr. Finesmith.

Part of the affidavit indicates that the inquiry will lead to evidence tending to show the identity of the user who accessed the defendant's doc ISP electronic mail account on the date in question on the defendant's laptop computer, provide information as to the person authorized to

access the electronic mail, provide information as to the identity of user of the laptop on January 23rd.

[The] State provided sufficient information to establish probable cause for the issuance of the CDW. It's apparent from the investigation that the medical websites were accessed on January 23rd, sites that would probably only be of interest to a medical doctor. [The] State is attempting to obtain the evidence with regard to that to further their investigation. Certainly Rules of Discovery required that the information be disclosed.

I do also find that the scope is excessive. The timeframe is very excessive, and I'm going to narrow the scope with regard to the inquiry [to] a timeframe prior to the seizure of the computer on January 27, 2005. I understand the State's problem to establish a course of conduct as to who would access this particular site. If there is only one access within a timeframe prior the question is still open as to who would seek access to that particular site. On the other hand, if there's a course of conduct that is relevant to the case to establish who was using that site, it might be quite relevant to further the investigation to disclose who was on the computer on the date in question. So with regard to the timeframe, I'm going to expand the timeframe to a fourteen-day period prior to the 27th which makes it January 13. So during that two-week timeframe, it will be able to show who was accessing and using that particular site. So, I'll modify the request to that timeframe.

On May 21, 2008 we granted the State's motion for leave to appeal from the two-week limitation of the CDW imposed by the

trial court. Defendant did not seek leave to appeal from the issuance of the CDW.

The State argues that the fourteen-day limit placed on the CDW unduly and erroneously restricts the State's investigation into the identity of the user of the DocISP account who possessed and made available child pornography on January 23, 2005, because the timeframe is insufficient to show a pattern of use of the account and fails to consider that within that timeframe defendant may not have used the DocISP account in his usual manner. In response, defendant claims the trial judge properly limited the State's overly broad application for a CDW.

Under the New Jersey Wiretapping and Electronic Surveillance Control Act, a CDW is different from a wiretap order in both the nature of the communication to which it is addressed and the standard for its issuance. A wiretap order permits the interception by law enforcement of a communication contemporaneous with the transmission while a CDW is directed to acquisition of communications in post-transmission electronic storage kept by an electronic communication service or remote computing service for reasons of backup protection for the communication. N.J.S.A. 2A:156A-2 to 156A-29; White v. White, 344 N.J. Super. 211, 220 (Ch. Div. 2001); see generally Fraser v. Nationwide Mut. Ins. Co., 35 F. Supp.2d 623, 633-34 (E.D. Pa.

2001); Fishman and McKenna, Wiretapping and Eavesdropping, supra, § 2.5. By definition, an electronic communication in storage cannot be "intercepted" because it is not contemporaneous with the transmission.⁴ See Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); Wesley Coll. v. Pitts, 974 F. Supp. 375, 389 (D. Del. 1997), aff'd o.b., 172 F.3d 861 (3rd Cir. 1998); Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996).

As a result, a CDW is not subject to the more restrictive procedures and enhanced protections of the Wiretap Act, which include a showing of necessity because normal investigative procedures have failed, N.J.S.A. 2A:156A-10. Instead, the statutory standard for a CDW requires only a showing of "reasonable grounds to believe that the record or other information pertaining to a subscriber or customer of an electronic communications server is relevant and material to an ongoing criminal investigation." N.J.S.A. 2A:156A-29A(e).

⁴ N.J.S.A. 2A:156A-2 defines "electronic storage" as follows:


- (1) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic submission thereof; and (2) any storage of such communication by an electronic communication service for purposes of backup protection of the communication.

In granting the CDW, the trial judge properly found that the information sought by the State was relevant and material to its investigation. However, the court's restriction of the CDW to the two-week timeframe was arbitrary since no reason was given for the limitation other than labeling the State's request "excessive" without any basis in the record to substantiate that conclusion.

Because the State seeks to show a pattern of use of defendant's DocISP account, a longer period than two weeks is appropriate for the State's investigation into the identification of the person who downloaded child pornography onto the laptop computer. We find no grounds to deny the State's requested period of one year as a reasonable timeframe for its investigation.

Reversed.

I hereby certify that the foregoing
is a true copy of the original on
file in my office.


CLERK OF THE APPELLATE DIVISION