IN THE SUPREME COURT OF THE STATE OF DELAWARE

CHRISTOPHER WHEELER,	)	
	)	
Defendant Below,	)	
Appellant,	)	
	)	
v.	)	No. 205, 2015
	)	
STATE OF DELAWARE,	)	
	)	
Plaintiff Below,	)	
Appellee.	)	

ON APPEAL FROM THE SUPERIOR COURT OF THE STATE OF DELAWARE IN AND FOR NEW CASTLE COUNTY

BRIEF OF THE AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF DELAWARE AS AMICUS CURIAE, URGING REVERSAL OF THE SUPERIOR COURT DECISION DENYING DEFENDANT'S MOTION TO SUPPRESS FILED AGAINST THE STATE

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF DELAWARE
Richard H. Morse (ID No. 531)
100 W. 10th St., Suite 603
Wilmington, DE 19801
(302) 654-5326
rmorse@aclu-de.org

Attorney for Proposed Amicus Curiae

August 26, 2015

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

STATEMENT OF INTEREST

Proposed Amicus Curiae, the American Civil Liberties Union Foundation of Delaware ("ACLU of Delaware"), submits this brief in support of appellant, defendant below, to urge reversal of the Superior Court decision denying the motion to suppress. The issues addressed by this brief are whether the Fourth Amendment to the United States Constitution and Art. I, § 6 of the Delaware Constitution require that a search warrant for electronic data be limited to those devices used during the time period in which the relevant data is believed to have been created or recorded, and whether a search for particular digital data may proceed by examining all digital data in the seized devices, regardless of the availability of less invasive means that would permit limiting the search to data for which probable cause exists. The prospect of warrants for all of a person's electronic data when there is only probable cause to search some of the person's data raises profound questions about Delawareans' right to be free from unreasonable searches and seizures in an ever more technologically capable society.

ACLU of Delaware has worked since 1961 through legal advocacy, engagement in the legislative process and public education to support the right of privacy. It most recently filed an amicus brief on Fourth Amendment issues in *State v. Holden*, No. 30, 2011.

ACLU of Delaware is a state affiliate of the American Civil Liberties Union ("ACLU"), a nonprofit, nonpartisan, 400,000 member organization founded in 1920 to protect and advance civil liberties throughout the United States. It promotes the constitutional and democratic values of free expression, privacy and liberty in a digital world. As part of this effort, its attorneys have filed numerous amicus briefs and briefs on behalf of parties in cases involving electronic surveillance and privacy issues including *Riley v. California*, 134 S. Ct. 2473 (2014) (amicus); *Clapper v. Amnesty Int'l USA,* 133 S. Ct. 1138 (2013) (counsel for appellee)*; United States v. Jones*, 132 S. Ct. 945 (2012) (amicus).

The motion to file this brief has been approved by ACLU-DE's Legal Review Panel.

ARGUMENT

Amicus submits this brief to challenge the scope of the warrants at issue in this case. For the purposes of this brief, Amicus accepts the decision of the court below to issue those warrants. Amicus limits its argument to the failure of the issuing judge to limit the warrants as required by the Fourth Amendment of the United States Constitution, Article I, § 6 of the Delaware Constitution and 11 *Del. C.* § 2307, and the failure of the trial judge to grant the motion to suppress.

In October of 2013, as part of a witness tampering investigation relating to communications that started in July 2013 (A26 ¶2, A27-28 ¶10-20), the state requested and obtained warrants authorizing the search of computers, cell phones, and other digital storage devices in the possession of Defendant Christopher Wheeler.

To obtain those warrants, the state submitted two affidavits of probable cause describing the events of July 2013 that gave rise to the investigation. A24-30, A36-43.[1] The affidavits stated that the state was searching for "evidence of written communications," A29, which it believed were relevant to the alleged witness tampering. 11 *Del. C.* §§1263(3), 3532.

[1] The affidavits of probable cause are identical except that one refers to defendant's residence and the other refers to his office, and the affidavit regarding his office has three additional paragraphs explaining that his desktop computer there may contain evidence of communications. For ease of reference, since the differences are not material to the legal issues, we cite only the affidavit that refers to the residence.

The affidavits indicate that the alleged witness tampering occurred, if it did, in or after July 2013, since that was when the witnesses and defendant renewed contact after a lengthy hiatus. A10. The affidavits contain no facts indicating that the alleged tampering might have occurred before then. Nevertheless, the warrants drafted by the investigators were unlimited as to time, and the issuing judge approved the warrants as drafted. A19-44.

Also, although the affidavits stated that the investigators were looking for evidence of written communications (A25),[2] the investigators requested and the court approved a warrant authorizing seizure of "any and all data … on any items seized" and the seizure of all "systems capable of storing digital or optical data" of any kind, including computers and cellphones. A19. Allowing the seizure of types of evidence beyond evidence of written communications, the warrants expressly authorized the search for and seizure of pictures, images, video recordings, and passwords. A19.

Proceeding under those warrants, an investigator, who determined that a computer he was starting to search had last been used in September 2012,

---

[2] The investigator wrote in his forensic report and testified that he was "exclusively" to be "looking for any files created and/or saved as word documents, emails, text messages, pdf or any other related file format" (A191). The sole portions of the affidavit of probable cause discussing the items sought for the criminal investigation discusses written communications, stating that "evidence of that correspondence may be in the residence and his workplace," "documents created by the user can be recovered through computer examination," and "e-mails and other electronically stored communications may be stored or maintained on the computer hard drive." A29. All reinforce that the items for which there was putatively probable cause to search and seize were written communications.

continued searching the computer even though it could not have contained material created or recorded during the relevant time period. A193. The investigator, Sgt. Perna did not limit his search to one that would have located only the text-based documents that he described as the proper scope of his search. A191, 194-95. Instead, he merely began opening directories and examining all of the files inside. A194-95. As the result of the nature of that search, he found a list of all files including video and image files. A195. That, in turn, led ultimately to seizure of the video files that led to defendant's indictment. A195.

The forensic examination could have searched only for "files created and/or saved as word documents, emails, text messages, pdf or any other related file format" for which he was "exclusively" looking and that did not disclose the list of video and image files. A193-94. The record contains some disagreement between Sgt. Perna and a defense forensic expert over the limitations of the forensic software employed by Sgt. Perna as to searching for keywords within different kinds of documents. Critically, however, both Sgt. Perna and the forensic expert testified that at a minimum Perna could have segregated video and image files from his search, and that even if the user had manipulated text-based files to show as image files in an attempt to conceal them from such a search (e.g., by changing the file extension) Sgt. Perna's forensic software would have alerted him to that fact. A197, A200. Nothing in the record supports the contention that it was

necessary for Sgt. Perna to view a list of all filenames in order to appropriately conduct his search for written communications.

The Fourth Amendment's particularity requirement required application of a technique that would have avoided reviewing data other than communications. Had the warrant contained a limitation consistent with the Fourth Amendment's requirement, the investigation would not have found the evidence used against defendant at trial. The issuing judge erred by approving a warrant that was insufficiently tailored to comply with the Fourth Amendment, see cases cited *infra* at 7-14, and the trial court therefore erred by denying defendant's motion to suppress. *See Wilson v. State*, 314 A.2d 905, 908 (Del. 1973) (holding that evidence derived from an invalid warrant should have been excluded at trial as "fruit of the poisonous tree").

The trial court rejected defendant's argument that the search was overly broad because it found that the disputed evidence was "located where a person with the type of training and experience possessed by Sergeant Perna might expect to find word documents or .pdf formatted documents" and because defendant "did not produce any evidence that Sergeant Perna's search approach (even absent the use of filters), and subsequent opening of the 'desktop' file folder, violated any recognizable search protocol or [the] like." Opinion on Motion to Suppress

(Exhibit A to Defendant's Opening Brief) at 18. That may be factually correct, but it is legally irrelevant to the validity of the warrant.

The court's reasoning ignored the question of whether it was legally proper for Sgt. Perna to conduct his search by simply opening a directory and viewing all the files without using any of the filtering or keyword searching functions available to him. Regardless of the technological choices Sgt. Perna had, the Fourth Amendment's particularity requirement barred issuance of any warrant that failed to limit the available techniques he could use to those that avoided unnecessary intrusions upon privacy that were not supported by probable cause. When a more targeted search is both feasible in the computer search context and justified by the nature of the probable cause, it is required. *See infra* at 11-14.

A. The Fourth Amendment Forbids Unconstrained Searches

The Fourth Amendment requires that "no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.[3] These restrictions are "the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed

[3] Del. Const., Art. I § 6 has a similar requirement ("no warrant to search any place, or to seize any person or thing, shall issue without describing them as particularly as may be"), as does 11 *Del. C.* § 2307 ("The warrant shall designate the … the things or persons sought as particularly as possible").

British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. ____, ____, 134 S. Ct. 2473, 2494 (2014). *See also Stanford v. Texas*, 379 U.S. 476, 481 (1965) (holding that the Fourth Amendment reflects the Framers' antipathy toward the evils of general warrants, as well as writs of assistance, which authorized British customs officials stationed in the Colonies to conduct broad, generalized searches of private homes at their discretion, in search of any goods that may have been imported in violation of English tax laws); *Ashcroft v. al-Kidd*, 563 U.S. ____, ____,131 S. Ct. 2074, 2084 (2011) ("The Fourth Amendment was a response to the English Crown's use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown.").

The warrant requirement addresses the Framers' concerns in two ways. "First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Second, the warrant requirement ensures that "those searches that are deemed necessary are as limited as possible," as the evil of unrestrained searches "is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." *Id.*

This latter goal is achieved by enforcing the particularity requirement of the Fourth Amendment's text. "By limiting the authorization to search to the specific

areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). *See also Marron v. United States*, 275 U.S. 192, 195-196 (1927) (stating that "[t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

Courts have routinely invalidated warrants whose "description . . . of the place to be searched is so vague that it fails reasonably to alert executing officers to the limits of their search authority." *United States v. Clark*, 638 F.3d 89, 94 (2d Cir. 2011); *see also United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002) ("The warrant must also describe the things to be seized with sufficient particularity and be no broader than the probable cause on which it is based."); *Davis v. Gracey*, 111 F.3d 1472, 1479 (10th Cir. 1997) (explaining that warrants are invalid "where the language of the warrants authorized the seizure of virtually every document that one might expect to find in a . . . company's office, including those with no connection to the criminal activity providing the probable cause for the search") (internal quotation omitted); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (invaliding warrant where warrant

"contained no limitations on what documents within each category could be seized or suggested how they related to specific criminal activity"). *See also Andresen v. Maryland*, 427 U.S. 463, 482 n. 11 (1976) (holding that the "State was correct in returning [papers that were not within the scope of the warrants or were otherwise improperly seized] voluntarily [to the owner]," and that the "trial judge was correct in suppressing others").

Recognizing the "grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable," *id.* 482 n. 11, *Andresen* cautioned that, when faced with searches and seizures of this scope, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Id.*

B. The Particularity Requirement is Heightened in the Context of Computer Searches

The dangers recognized by *Andresen* are particularly present in the execution of warrants addressing digital information, where a search will implicate not only great volumes of "papers," but an unprecedented diversity of private information as well. *See Riley*, 134 S. Ct. at 2489 ("[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement,

a video—that reveal much more in combination than any isolated record. [And] a cell phone's capacity allows even just one type of information to convey far more than previously possible.").[4]

The search of a digital device "would typically expose to the government far *more* than the most exhaustive search of a house." *Riley*, 134 S. Ct. at 2491. For this reason and because "computers and email accounts often contain significant intermingling of relevant documents with documents that the government has no probable cause to seize," the particularity requirement of the Fourth Amendment has taken on renewed importance in the digital age. *United States v. Ali*, 870 F. Supp. 2d 10, 39 (D.D.C. 2012) (internal quotation marks and citations omitted); *accord United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (when "the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance.").

[4] Noting that modern cell phones are capable of storing a vast amount of personal information and thus deserve the highest privacy protections, *Riley* held that cell phones may not be searched under the search-incident-to-arrest warrant exception. 134 S. Ct. at 2491. While *Riley* formally considered "cell phones," the Court made clear that its analysis was really about computers generally, not just computers that allow voice transmission and are therefore called phones. *See id*. at 2489 ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."). For Fourth Amendment purposes there is no difference between a computer and a smart phone.

C. The Warrant in this Case Was Overbroad and Violated the Particularity Requirement Because it Had No Temporal Limitation and Did Not Require Investigators to View Only Those Files that were Potentially Responsive

The particularity requirement restricts proper computer searches to devices that may contain files created or modified within the time period whose relevance is supported by the affidavit of probable cause. *See United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) (stating that failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad) (internal citation and quotation omitted); *Kow*, 58 F.3d at 427 (finding overbreadth when "[t]he government did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place"); *United States v. Abrams*, 615 F.2d 541, 545 (1st Cir. 1980) (invalidating warrant for failure to place time frame on documents seized and examined). *Cf. United States v. Evaschuck*, 65 F. Supp. 2d 1360, 1366 (M.D. Fla. 1999) (finding that agents should not have searched logbooks that they knew contained "only documents that predated the time frame specified in the search warrant").

The warrants that led to discovery of the evidence were not limited to a time period supported by probable cause. Those warrants had no time limitation at all (see A19-20, A31-32), and that lack of the required time limitation necessitates reversal of Superior Court's denial of the motion to suppress, since its absence led to discovery of the evidence. Even though Sgt. Perna determined at the outset of

his search that the computer he was searching could not have contained data from 2013, he nevertheless proceeded under the authority of the warrant to examine it. It was that improper search that ultimately led to the defendant's indictment.

Reversal of the decision on the motion to dismiss is also required because the warrant did not limit the search to the data for which there was probable cause, the communications data Sgt. Perna understood he was to look for. A191. Instead, it permitted a search for "any and all data." A19.

In the computer context, the particularity requirement also limits the scope of the examination of particular files or data to that for which there is probable cause that the evidence sought will be found therein. *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005) (holding a warrant authorizing seizure of all storage media and "not limited to any particular files" violated the Fourth Amendment); *Klitzman, Klitzman & Gallagher v. Krut*, 744 F.2d 955, 960 (3d Cir. 1984) (finding that search and seizure of all of law firm's records was improper when only a portion of the firm's records were allegedly involved in criminal activity); *United States v. Fleet Mgmt. Ltd.*, 521 F. Supp. 2d 436, 444-445 (E.D. Pa. 2007) (holding that a warrant permitting the seizure of "any and all data"

constituted an improper "general warrant" when there was sufficient information to provide for a more targeted search and seizure).[5]

The absence of required limitation on what could be searched, which was necessary to prevent searches for the data for which there was no probable cause, presents a second reason why reversal is required. Both the investigator and the forensic expert agreed that the software then in use was capable of filtering out images and videos from the search and alerting the investigator if the user had attempted to conceal text documents therein by altering files. A197, A200. Because there was no lawful basis for the investigator to view the image and video filenames, the resulting evidence should have been suppressed. *Horton v. California*, 496 U.S. 128, 136 (1990) (holding that the plain view doctrine only

---

[5] There are two Delaware Supreme Court cases addressing the issue of whether searches of computer files did not properly restrict the viewing of files known to be unresponsive, but neither is applicable here. In *State v. Fink*, 2001 Del. Super. LEXIS 188 (Del. Super. Ct. Mar. 30, 2001), in contrast to the evidence presented in this case as to the feasibility of a narrow search based on sophisticated forensic software, the Superior Court found based on the evidence in that case that "in order to conduct a complete search for particular evidence in a computer, it may be necessary to take a look at the contents of every file." 2001 Del. Super. LEXIS 188, *8. And, in any event, Fink never appealed the March 30, 2001 suppression decision as to the warrant that involved the method of search (the second of the three warrants), so this Court never had the opportunity to consider the proper method of searching digital files when only text-based files are sought. *Fink v. State*, 817 A.2d 781, 786 (Del. 2003). In *Bradley v. State*, 51 A.3d 423 (Del. 2012), the defendant had argued that it was improper for the investigator to view video files when the warrant authorized the search for patient records, but the Court found both that patient files often include multi-media, and that the affidavit of probable cause provided a clear basis for seeking pictures and video since the allegation was that "Bradley installed surveillance cameras throughout his office, which he could observe from home, and that he took images of patients which he then manipulated on his home computer." 51 A.3d at 435 (Del. 2012). Thus, in *Bradley*, there was no basis for segregating text files from other types of files because the probable cause allowed for the search for both.

applies when "the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed").

D. Conclusion

The Supreme Court has cautioned against allowing new technologies "to erode the privacy guaranteed by the Fourth Amendment." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). *See also United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2001) ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.") (citing *Kyllo*). The Supreme Court recognized this problem again in *Riley*, reasoning that Fourth Amendment privacy protection must account for the new technological reality.

This case shows the truth of those observations. The concerns animating *Riley, Andresen* and the decisions cited *supra* at 7-14 apply equally here and call upon this Court to reverse Superior Court's denial of the motion to suppress. The state must act pursuant to a warrant that comports with our constitutions when it searches digital data. It did not do so here, so reversal is required. ACLU-DE recognizes the deference that this Court grants lower courts with regard to the issuance of search warrants. *See, e.g., State v. Holden*, 60 A.3d 1110, 1114 (Del. 2013). But this is not the kind of case in which this Court is being asked to second-guess some potentially reasonable judgment call about the facts, or apply some overly technical burden on the lower court, which are the

concerns animating the deference doctrine. *See id.* (describing need to defer to reasonable, fact-bound determinations of probable cause and to avoid hyper-technical parsing). Instead, this case involves the absence of any justification whatsoever for a search that included image files from 2012 in an investigation into written correspondence from 2013. In this matter, there was a clear violation of the Fourth Amendment and Article I, § 6.

While it may be difficult to suppress evidence that an educator has been in possession of child pornography, "[i]t is a fair summary of history to say that the safeguards of liberty have frequently been forged in controversies involving not very nice people." *United States v. Rabinowitz*, 339 U.S. 56, 69 (1950) (Frankfurter, J. dissenting). Suppression is required to keep the Fourth Amendment and Article I, § 6 viable in our electronic age.

/s/ Richard H. Morse
Richard H. Morse (ID No. 531)
American Civil Liberties Union Foundation
of Delaware
100 W. 10th St., Suite 603
Wilmington, DE 19801
(302) 654-5326
rmorse@aclu-de.org
Attorney for Proposed Amicus Curiae

August 26, 2015